CUSEC

Základy regulácie kybernetickej bezpečnosti a súvisiacich oblastí

Modul 2 - Základy právnej úpravy kybernetickej bezpečnosti
Časť 1

Doc. JUDr. Jozef Andraško, PhD.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality
CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

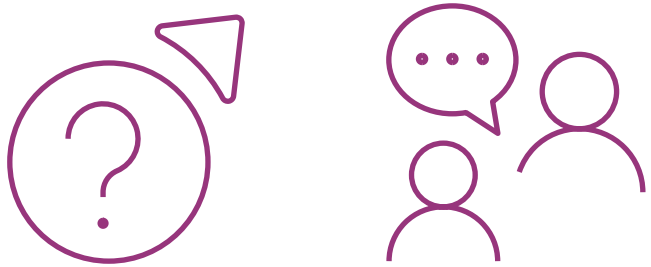
Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované
Európskou úniou
NextGenerationEU

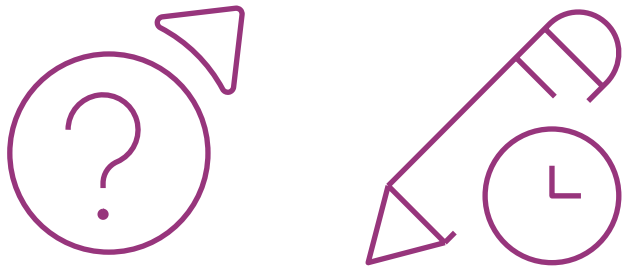
PLÁN OBNOVY

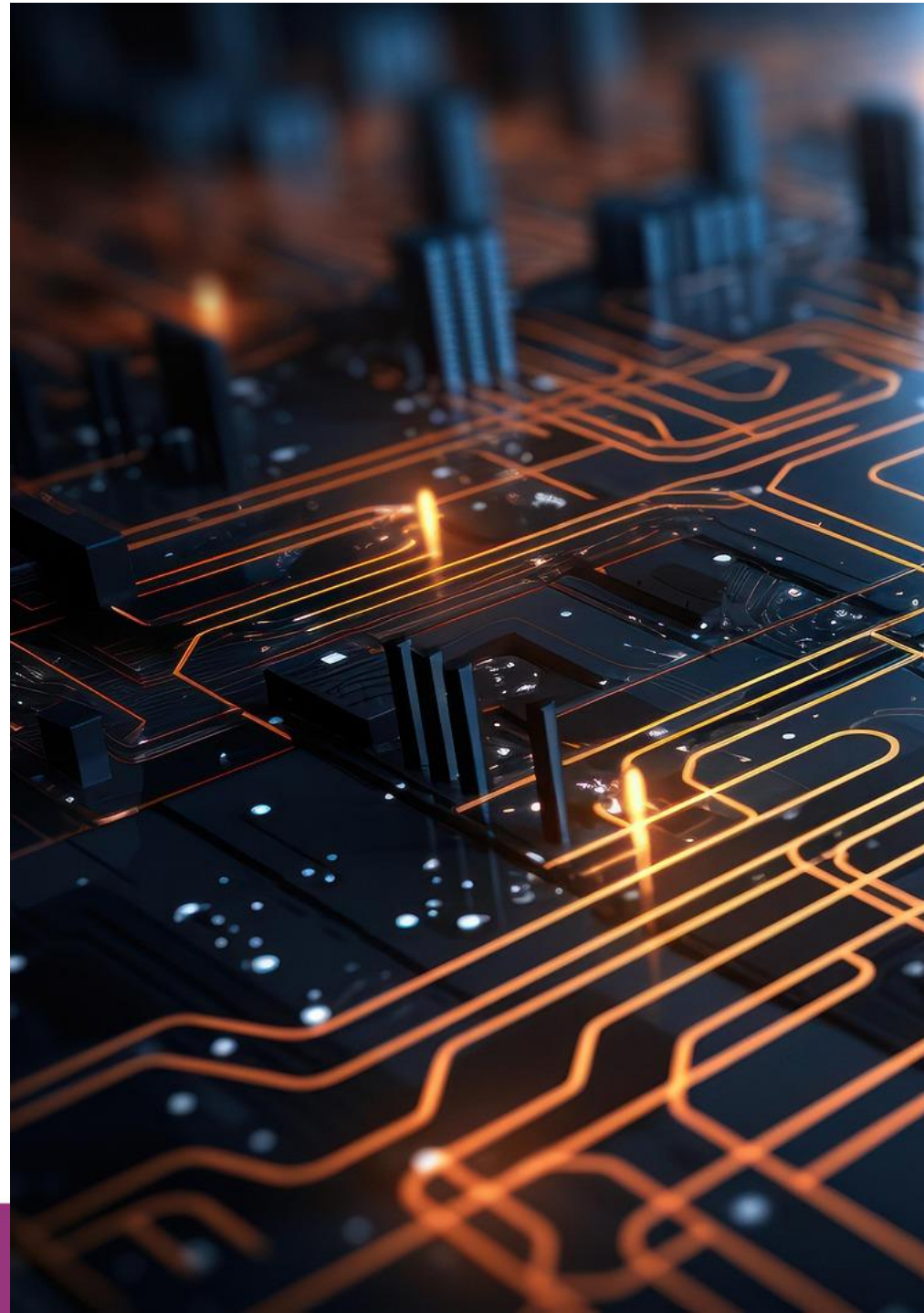
MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Koho regulovať?



Aké sektory sú podľa vás najdôležitejšie?





- Technologická neutralita
- Ochrana informačného sebaurčenia človeka
- Ochrana nedistributívnych (verejných) práv
- **Minimalizácia štátneho donútenia**
- Autonómia vôle regulovaných subjektov
- Bdelosť vo vzťahu k ostatným štátom

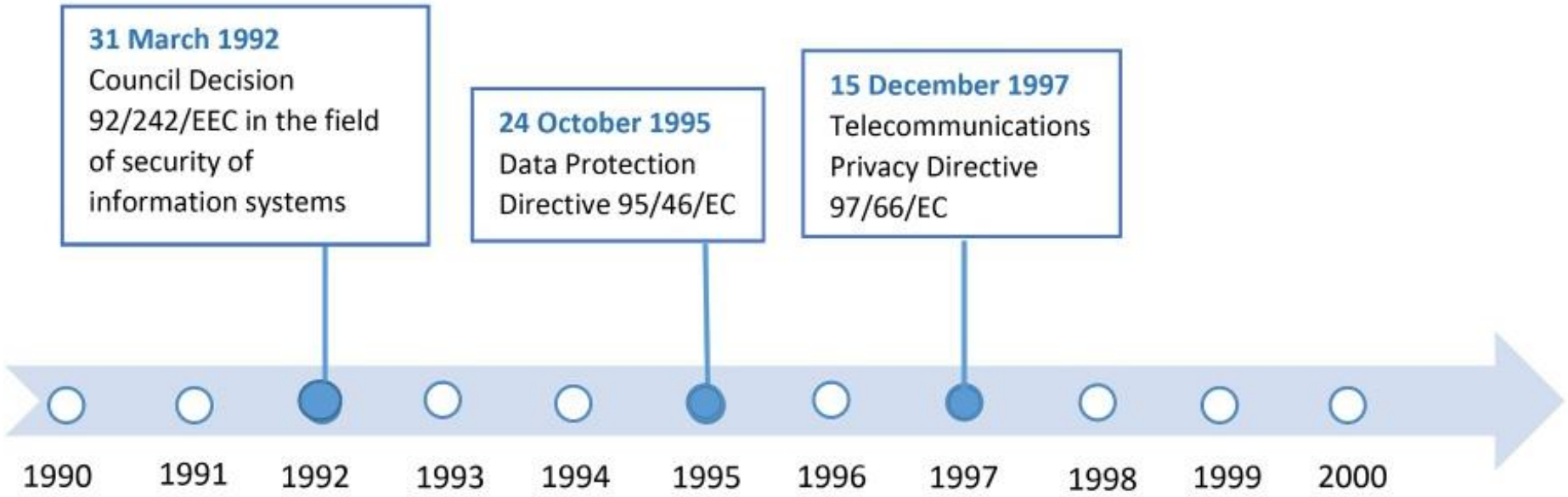


Fig. 1. Legislative enactments 1990–2000.

CUSEC

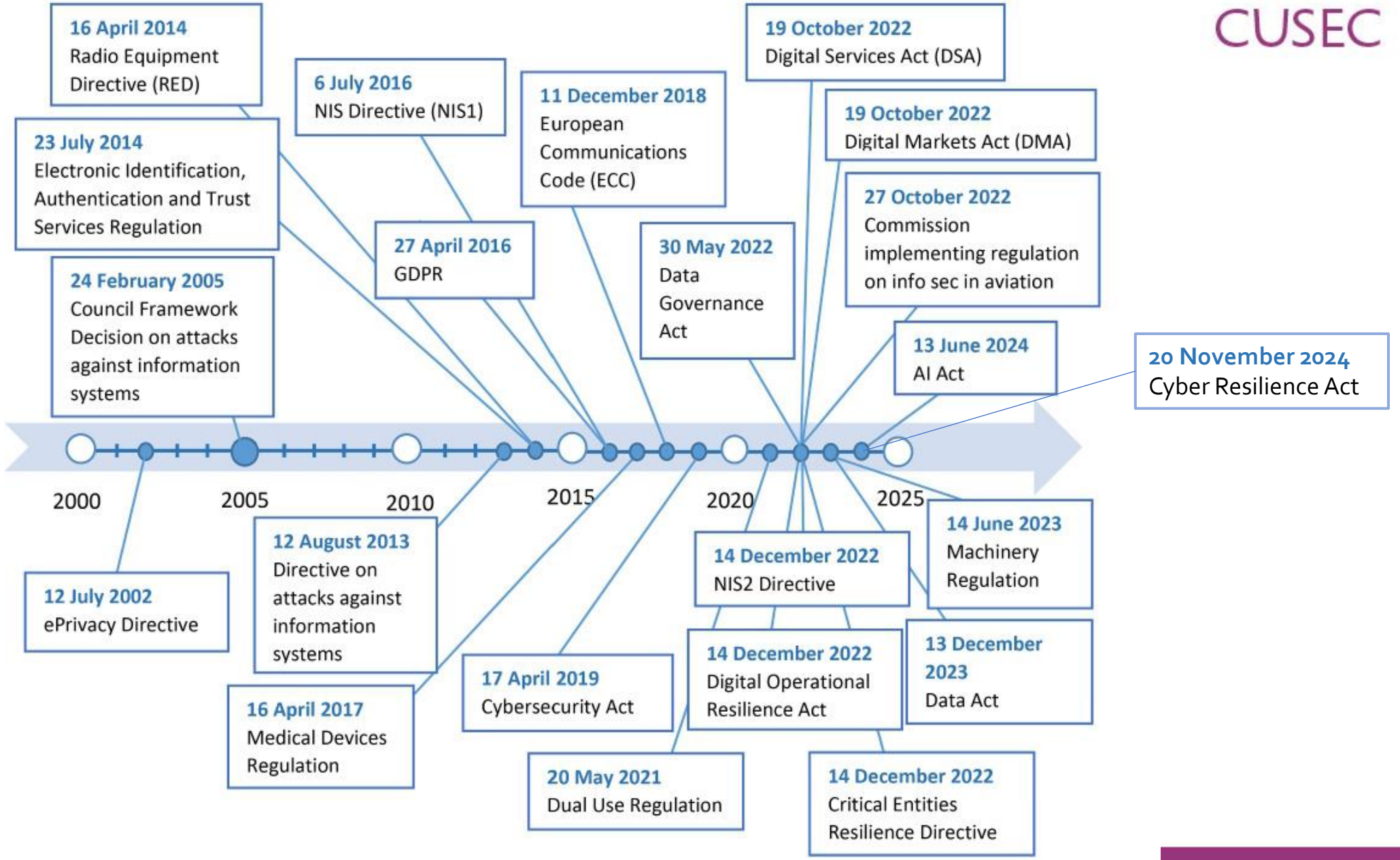


Fig. 2. Legislative enactments 2000–2024.

CUSEC

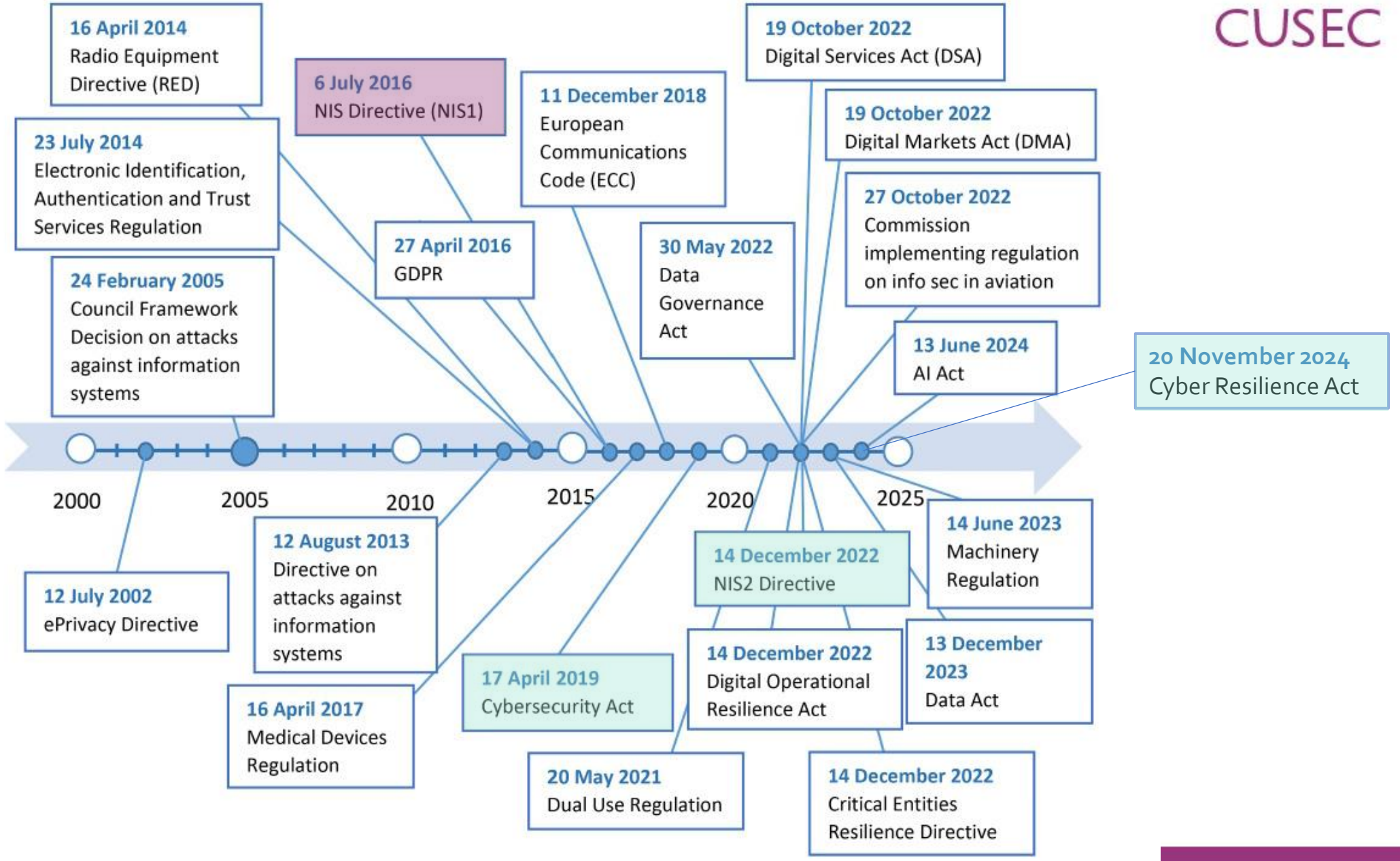
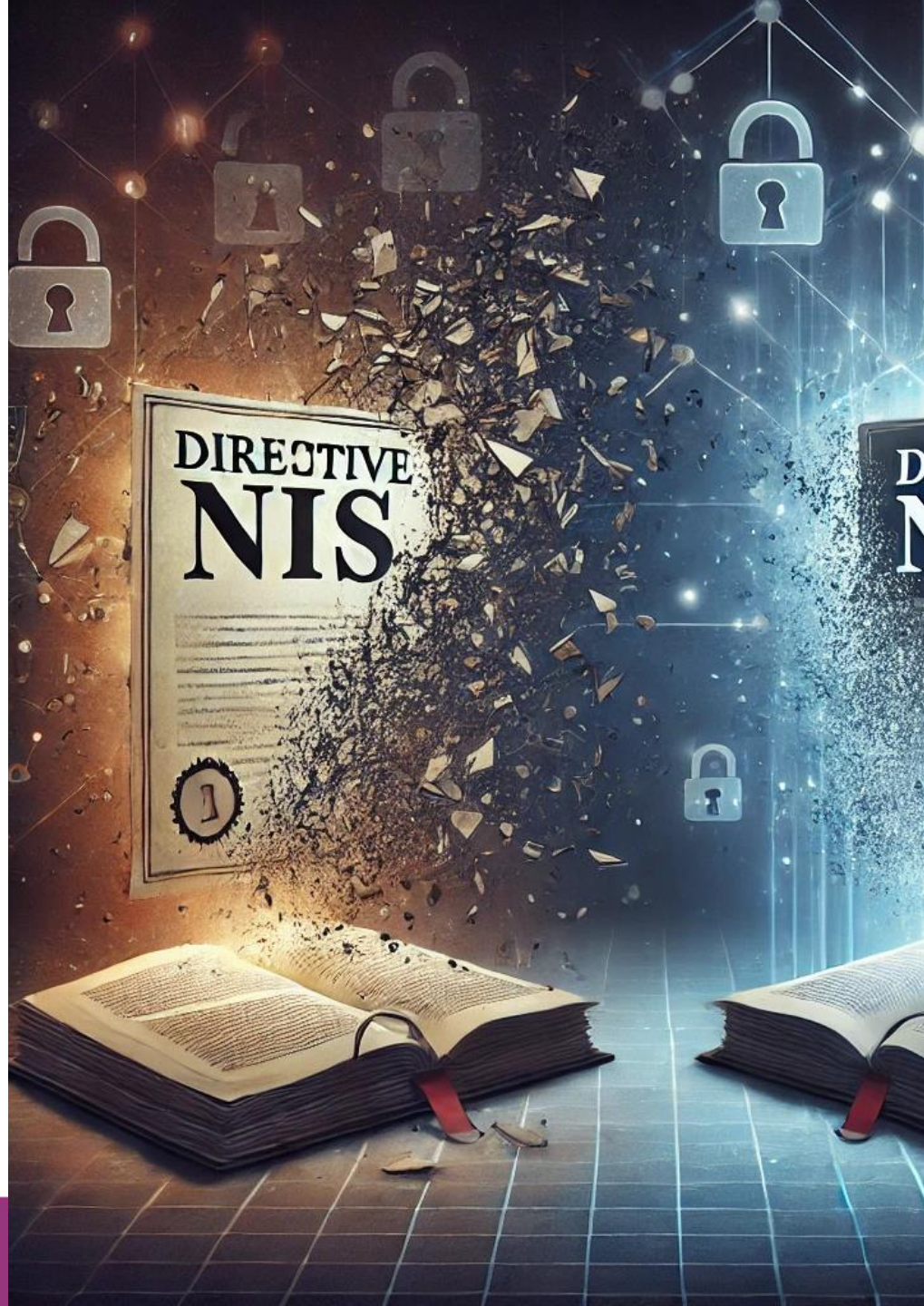


Fig. 2. Legislative enactments 2000–2024.

- 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



CUSEC

Smernica NIS – predmet úpravy a pôsobnosť

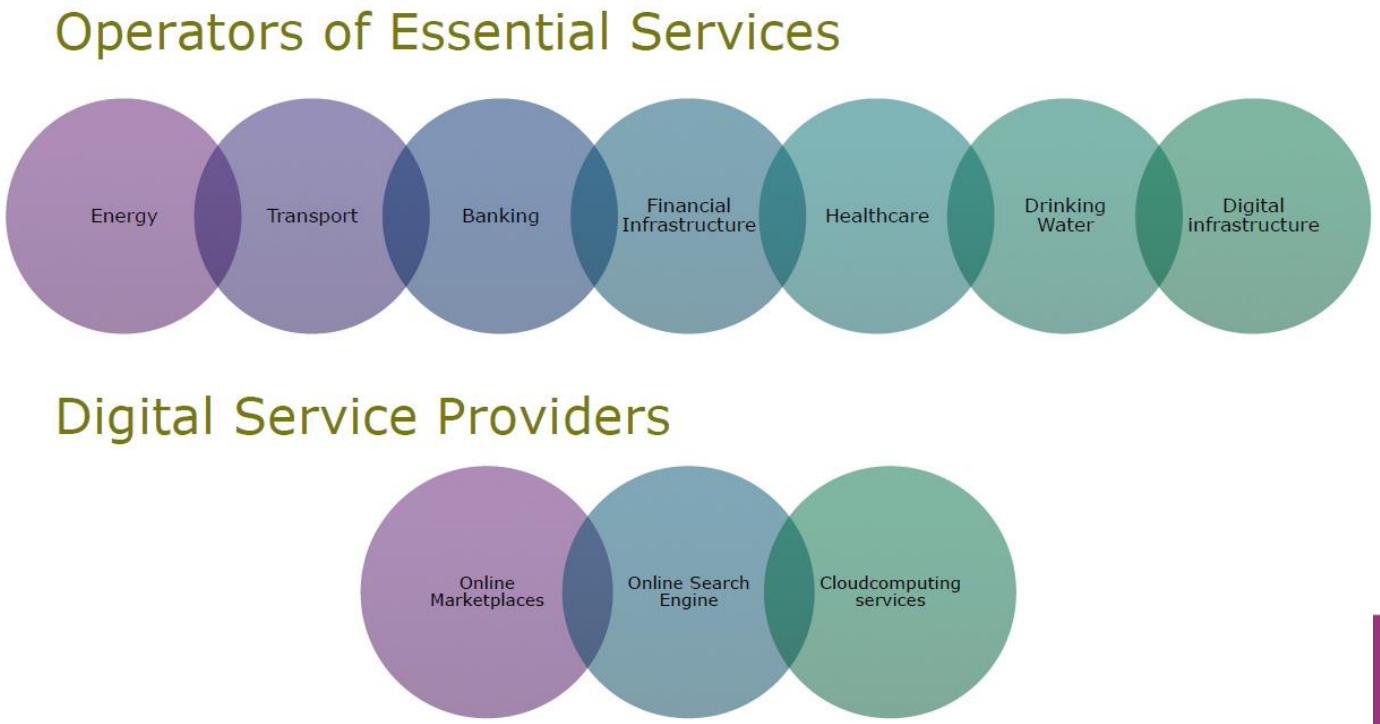
- opatrenia na dosiahnutie **vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov** v rámci EÚ s cieľom zlepšiť **fungovanie vnútorného trhu**.

Smernica NIS – PZS a PDS

zásada minimálnej harmonizácie (2 aspekty)

CUSEC

- kľúčové hospodárske subjekty:
  - **prevádzkovatelia základných služieb** a
  - **poskytovatelia digitálnych služieb**



Smernica NIS – povinnosti

Performatívne pravidlá (performance-based rules)

1. Členské štáty zabezpečia, aby PZS **prijali vhodné a primerané technické a organizačné opatrenia** na **riadenie rizík** súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke.

2. Členské štáty zabezpečia, aby PZS prijali **primerané opatrenia na zabránenie a minimalizovanie vplyvu incidentov**, ktoré ovplyvňujú bezpečnosť sietí a informačných systémov používaných na poskytovanie týchto základných služieb, s cieľom zabezpečiť ich kontinuitu.

Smernica NIS – povinnosti

3. Členské štáty zabezpečia, aby PZS **bez zbytočného odkladu oznamovali** príslušnému orgánu alebo jednotke CSIRT **incidenty, ktoré majú závažný vplyv** na kontinuitu základných služieb, ktoré poskytujú.

- *„každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov.*"

- oznamujú sa len **závažné incidenty**

Prečo smernica NIS 2?

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 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**)

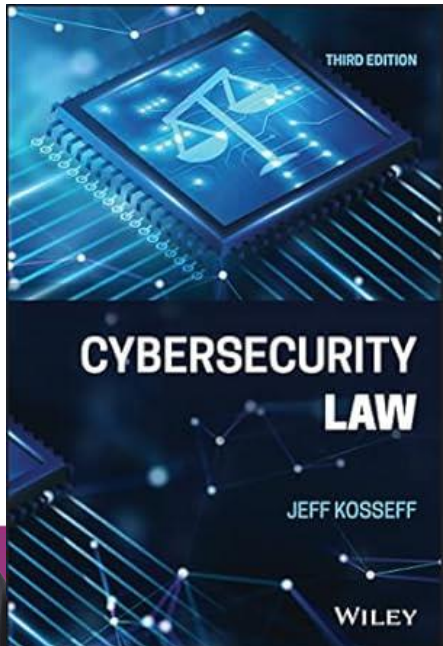
Spomeňte si na Jeffa Kosseffa

CUSEC

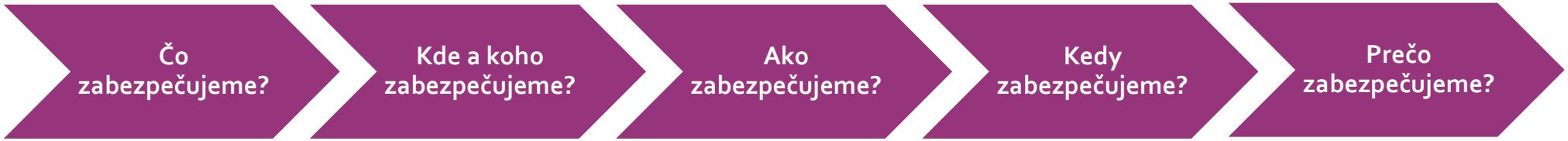
Právo kybernetickej bezpečnosti – pojem

- *„právny rámec, ktorý zabezpečuje dôvernosť, integritu a dostupnosť verejných a súkromných informácií, systémov a sietí prostredníctvom nadčasovej regulácie a stimulov, s cieľom chrániť práva a súkromie jednotlivcov, ekonomické záujmy a národnú bezpečnosť.“*

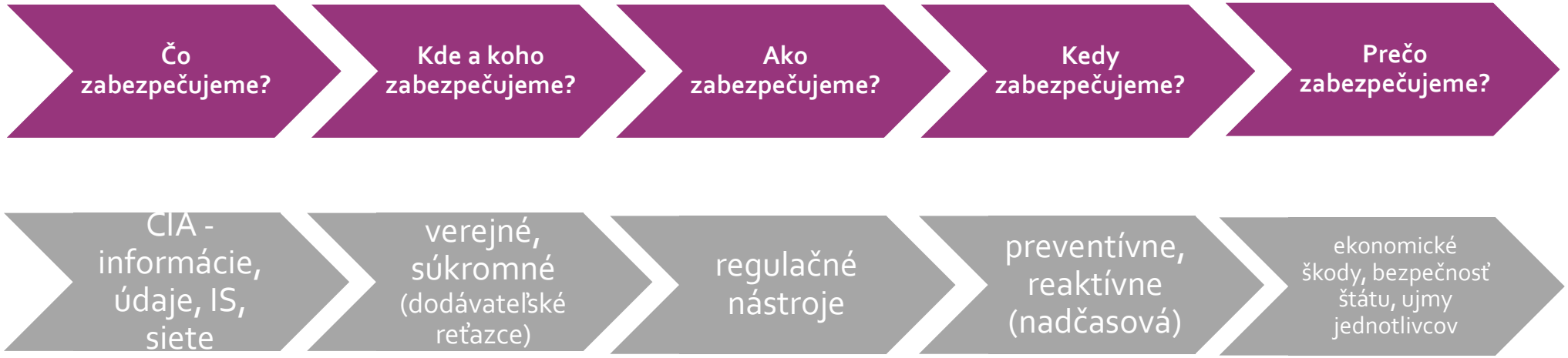
Jeff Kosseff
associate professor of cybersecurity law
United States Naval Academy's Cyber Science Department



CUSEC


Čo zabezpečujeme?
Kde a koho zabezpečujeme?
Ako zabezpečujeme?
Kedy zabezpečujeme?
Prečo zabezpečujeme?

CUSEC


Čo zabezpečujeme?
Kde a koho zabezpečujeme?
Ako zabezpečujeme?
Kedy zabezpečujeme?
Prečo zabezpečujeme?
CIA - informácie, údaje, IS, siete
verejné, súkromné (dodávateľské reťazce)
regulačné nástroje
preventívne, reaktívne (nadčasová)
ekonomické škody, bezpečnosť štátu, ujmy jednotlivcov

CUSEC

Čo a prečo?

Predmet úpravy

Smernica NIS 2 – predmet úpravy

- Touto smernicou sa stanovujú opatrenia, ktorých zámerom je **dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti** v celej Únii na účely **lepšieho fungovania vnútorného trhu.**

Smernica NIS
Touto smernicou sa stanovujú opatrenia na dosiahnutie vysokej spoločnej úrovne **bezpečnosti sietí a informačných systémov** v rámci Únie s cieľom zlepšiť fungovanie vnútorného trhu.

- **Kybernetická bezpečnosť?**

Smernica NIS 2

CUSEC

Authenticity is important to ensure that information and communication come from a trusted source. This includes protecting against impersonation, spoofing and other types of identity fraud. Common techniques used to establish authenticity include authentication, digital certificates, and biometric identification.

- **Bezpečnosť sietí a informačných systémov**

- *„schopnosť **sietí a informačných systémov** odolávať na určitom stupni spoľahlivosti akejkoľvek udalosti, ktorá môže ohroziť **dostupnosť, pravosť, integritu alebo dôvernosť** uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.“*

Smernica NIS

Smernica NIS 2

- **Siete a informačné systémy**

A	**elektronická komunikačná sieť**
B	každé **zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení**, z ktorých jedno alebo viaceré vykonávajú **automatické spracúvanie digitálnych údajov** na základe programu, alebo
C	**digitálne údaje**, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú **prostredníctvom prvkov** uvedených v písmenách a) a b) **na účely ich prevádzkovania, používania, ochrany a udržiavania**

Akt o kybernetickej bezpečnosti (nariadenie 2019/881)

CUSEC

SIS (NIS)

užívatelia

iné osoby

Kybernetická bezpečnosť

- „činnosti potrebné na **ochranu sietí a informačných systémov**, **užívateľov** takýchto systémov a **iných osôb dotknutých** kybernetickými hrozbami."

Kybernetická hrozba

- „každá potenciálna **okolnosť, udalosť alebo činnosť**, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť **siete a informačné systémy**, **užívateľov** takýchto systémov **a iné osoby**."

Prístup založený na právach

Otvorená definícia

CUSEC

Kde a koho?

Pôsobnosť

Pôsobnosť (čl. 2)

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

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

Nové sektory a podsektory

- pravidlo obmedzenia veľkosti (size-cap rule)
  - ***verejné alebo súkromné subjekty*** *typu uvedeného* ***v prílohe I alebo II,*** *ktoré sa považujú za* ***stredné podniky*** *podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo* ***presahujú limity*** *pre stredné podniky stanovené v odseku 1 uvedeného článku a ktoré poskytujú služby alebo vykonávajú svoje činnosti v Únii.*

mikropodniky | **malé podniky** | **stredné podniky** | **veľké podniky**

Pôsobnosť (čl. 2)

Mikropodniky

- *podniky, ktoré zamestnávajú menej ako **10 osôb** a ktorých ročný obrat alebo ročná bilančná suma nepresahuje **2 milióny eur***

Malé podniky

- *podniky, ktoré zamestnávajú menej ako 50 osôb a ktorých ročný obrat alebo ročná bilančná suma nepresahuje 10 miliónov eur.*

Stredné podniky

- *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.*

Veľké podniky

- *Za veľké podniky sa považujú podniky, ktoré zamestnávajú **250 a viac osôb** a ktoré majú buď ročný obrat prevyšujúci **50 miliónov eur**, alebo ročnú bilančnú sumu prevyšujúcu **43 miliónov eur**.*

CUSEC

Kategória podniku	Počet pracovníkov: ročná pracovná jednotka (RPJ)	Ročný obrat	alebo	Celková ročná bilančná suma
Stredné podniky	< 250	≤ 50 miliónov EUR	alebo	≤ 43 miliónov EUR
Malé podniky	< 50	≤ 10 miliónov EUR	alebo	≤ 10 miliónov EUR
Mikropodniky	< 10	≤ 2 milióny EUR	alebo	≤ 2 mil. EUR

Pôsobnosť (čl. 2)

Príloha I – ODVETVIA S VYSOKOU ÚROVŇOU KRITICKOSTI

- energetika,
- doprava,
- bankovníctvo,
- infraštruktúry finančných trhov,
- zdravotníctvo,
- pitná voda,
- odpadová voda,
- digitálna infraštruktúra,
- riadenie služieb IKT (medzi podnikmi)
- **verejná správa** a
- vesmír.

Pôvodný návrh smernice NIS 2 – Odvetvia pre kľúčové subjekty

— subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom
— subjekty verejnej správy na regionálnej úrovni, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom

CUSEC

Pôsobnosť (čl. 2)

Príloha II – INÉ KRITICKÉ ODVETVIA

- poštové a kuriérske služby,
- odpadové hospodárstvo,
- 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

- Táto smernica sa vzťahuje aj na **subjekty** typu uvedeného v **prílohe I alebo II** bez ohľadu na ich veľkosť, ak..... (a-f)

- **malé podniky a mikropodniky**, ktoré spĺňajú osobitné kritériá, ktoré naznačujú **kľúčovú úlohu** pre spoločnosť, hospodárstvo alebo pre určité odvetvia alebo druhy služieb, **patria do rozsahu pôsobnosti** Smernice NIS 2 (R 7)

Cesta k NIS 3

Pôsobnosť (čl. 2) – výnimky z POV

- Táto smernica sa vzťahuje aj na **subjekty** typu uvedeného v **prílohe I alebo II bez ohľadu na ich veľkosť**, **ak**.....

a) služby poskytujú:

   i) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb;

   ii) poskytovatelia dôveryhodných služieb;

   iii) registre názvov domén najvyššej úrovne a poskytovatelia služieb systému názvov domén;

b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností;

c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie;

d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte;

Pôsobnosť (čl. 2) – výnimky z POV

- Táto smernica sa vzťahuje aj na **subjekty** typu uvedeného v **prílohe I alebo II bez ohľadu na ich veľkosť**, **ak**……

- f) subjekt je **subjektom verejnej správy**:
  - i) v **ústrednej štátnej správe** podľa definície členského štátu v súlade s vnútroštátnym právom; alebo
  - ii) **na regionálnej úrovni** podľa definície členského štátu v súlade s vnútroštátnym právom, <u>ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti</u>.

CUSEC

Subjekt verejnej správy – čl. 6 bod 35

- subjekt, ktorý je ako **taký uznaný v členskom štáte** v súlade s vnútroštátnym právom, **okrem súdnictva, parlamentov a centrálnych bánk**, a ktorý spĺňa tieto kritériá:

a) je zriadený na účely plnenia **potrieb všeobecného záujmu** a nemá priemyselný ani komerčný charakter;
b) má **právnu subjektivitu** alebo je **zo zákona oprávnený konať** v mene iného subjektu s právnou subjektivitou;
c) je **financovaný** prevažne štátnymi, regionálnymi alebo inými verejnoprávnymi orgánmi, podlieha dohľadu týchto inštitúcií alebo orgánov nad svojím riadením alebo v správnom, riadiacom alebo dozornom orgáne má viac ako polovicu členov menovaných štátnymi alebo regionálnymi orgánmi alebo inými verejnoprávnymi inštitúciami;
d) má **právomoc vydávať** fyzickým alebo právnickým osobám **správne alebo regulačné rozhodnutia**, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovarov, služieb alebo kapitálu;

Pôsobnosť

- Členské štáty **môžu** ustanoviť, že sa Smernica NIS 2 vzťahuje na:
  - subjekty verejnej správy na **miestnej úrovni**;
  - **vzdelávacie inštitúcie**, najmä tie, v ktorých sa vykonávajú **kritické výskumné činnosti**.

Negatívna pôsobnosť

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

- SVS, ktorých činnosti s uvedenými oblasťami súvisia len okrajovo, by však nemali byť vylúčené z rozsahu pôsobnosti smernice NIS2

- sa nevzťahuje na subjekty, ktoré členské štáty vyňali z rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 (DORA) v súlade s článkom 2 ods. 4 uvedeného nariadenia

Kľúčové subjekty a dôležité subjekty

CUSEC

Kľúčové subjekty (čl. 3)

- Na účely Smernice NIS 2 sa za **kľúčové subjekty** považujú:
  - subjekty typu uvedeného **v prílohe I,** ktoré **presahujú limity** pre **stredné podniky** stanovené v článku 2 ods. 1 prílohy k odporúčaniu 2003/361/ES;
  - **kvalifikovaní poskytovatelia dôveryhodných služieb a registre názvov domén najvyššej úrovne,** ako aj poskytovatelia služieb DNS, **bez ohľadu na ich veľkosť;**
  - poskytovatelia **verejných elektronických komunikačných sietí** alebo verejne dostupných elektronických komunikačných služieb, ktoré sú považované za stredné podniky
  - **subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i);**

v ústrednej štátnej správe

CUSEC

Kľúčové subjekty (čl. 3)

- Na účely Smernice NIS 2 sa za **kľúčové subjekty** považujú:
  - akékoľvek iné subjekty typu uvedeného v prílohe I alebo II, ktoré členský štát označil za kľúčové subjekty podľa článku 2 ods. 2 písm. b) až e);
  - subjekty označené ako **kritické subjekty** podľa smernice (EÚ) 2022/2557 uvedenej v článku 2 ods. 3 tejto smernice;
  - ak tak členský štát ustanoví**, subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb** v súlade so smernicou (EÚ) 2016/1148 alebo vnútroštátnym právom.

CUSEC

Dôležité subjekty (čl. 3)

- Subjekty typu uvedeného v prílohe I alebo II**, ktoré sa nepovažujú za kľúčové** subjekty podľa odseku 1 článku 3 smernice NIS 2

- Patria sem subjekty **označené členskými štátmi ako dôležité** subjekty podľa článku 2 ods. 2 písm. b) až e) smernice NIS 2.

b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností;

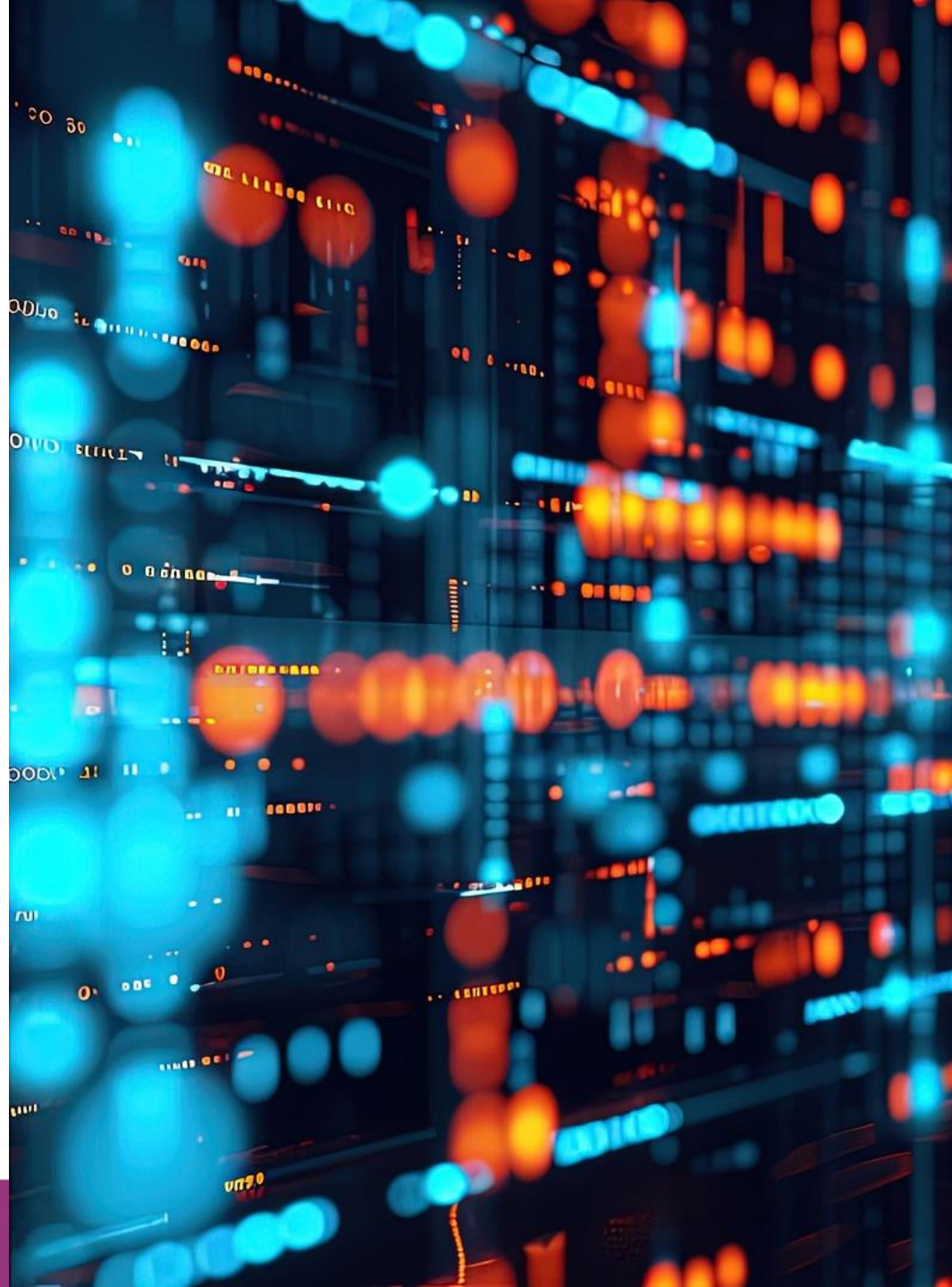
c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie;

d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte;

Do 17. apríla 2025 - zoznam kľúčových a dôležitých subjektov

Lex specialis - lex generalis



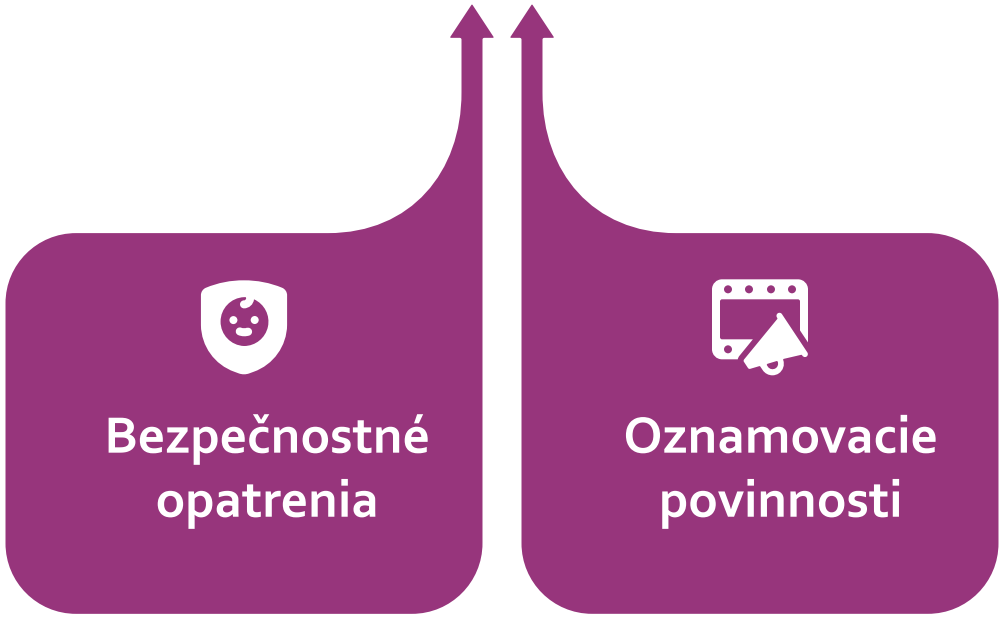
CUSEC

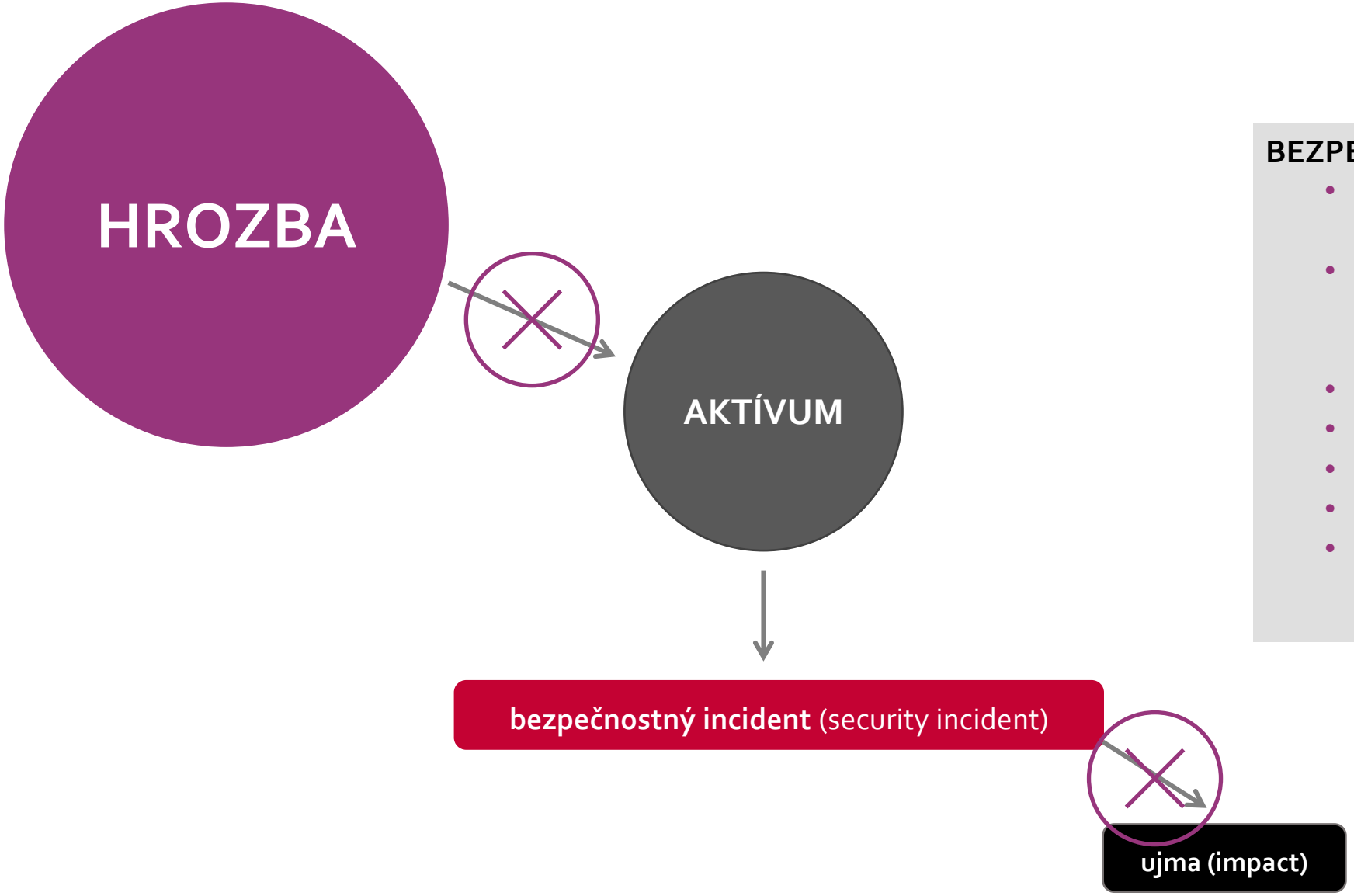
Odvetvové právne akty

- Ak sa v **odvetvových právnych aktoch** Únie vyžaduje, aby kľúčové alebo dôležité subjekty **prijali opatrenia na riadenie kybernetických rizík alebo aby nahlasovali významné incidenty,** a 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 VII sa na takéto subjekty **nevzťahujú.**

CUSEC

Ako a kedy?


Bezpečnostné opatrenia
Oznamovacie povinnosti



BEZPEČNOSTNÉ OPATRENIA

- minimalizovať riziko vzniku incidentu
- minimalizovať dopad incidentu

- záloha
- silné heslo
- šifrovanie
- školenie personálu
- manažér kybernetickej bezpečnosti

Opatrenia na riadenie kybernetických rizík

Riadenie (čl. 20)

- **<u>riadiace orgány</u>** kľúčových a dôležitých subjektov
  - **schválili opatrenia** na riadenie kybernetických rizík, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 21
  - **dohliadali** na jeho vykonávanie a
  - aby mohli **byť brané na zodpovednosť**, ak subjekty porušujú uvedený článok.

- nie je dotknuté vnútroštátne právo, pokiaľ ide o pravidlá zodpovednosti uplatniteľné na **verejné inštitúcie**

Riadenie (čl. 20)

- **<u>členovia riadiacich orgánov</u>** kľúčových a dôležitých subjektov **povinní**
  - absolvovať **odbornú prípravu**

- kľúčové a dôležité subjekty (povinnosť?)
  - svojim zamestnancom **pravidelne poskytovali** **podobnú odbornú prípravu** a ich zamestnanci tak získali dostatočné znalosti a zručnosti a vedeli rozpoznať riziká a posúdiť postupy riadenia kybernetických rizík a ich vplyv na služby poskytované subjektom

CUSEC

Opatrenia na riadenie kybernetických rizík (čl. 21)

- kľúčové a dôležité subjekty prijali **vhodné a primerané technické, operačné a organizačné opatrenia** na **riadenie rizík** súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na **prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov** ich služieb a na ďalšie služby

- opatrenia sú založené na **prístupe zohľadňujúcom všetky riziká**, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi

Opatrenia (čl. 21)

Vykonávacie akty, ktorými stanoví technické, metodické, ako aj odvetvové požiadavky na opatrenia

Výpočet od písm. **a) – j)**

a) zásady analýzy rizík a bezpečnosti informačných systémov
b) riešenie incidentov
c) kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie
d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb
e) bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach

Opatrenia (čl. 21)

f) zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík

g) základné postupy **kybernetickej hygieny** a odborná príprava v oblasti kybernetickej bezpečnosti

Opatrenia (čl. 21)

- R 49
- Politiky kybernetickej hygieny poskytujú **základy pre ochranu** infraštruktúry sietí a informačných systémov, bezpečnosť hardvéru, softvéru a online aplikácií a ochranu obchodných údajov alebo údajov o koncových používateľoch, na ktoré sa subjekty spoliehajú.
- Politiky kybernetickej hygieny zahŕňajúce spoločný **základný súbor postupov** vrátane aktualizácií softvéru a hardvéru, zmeny hesiel, riadenia nových inštalácií, obmedzenia prístupových účtov na úrovni správcu a zálohovania údajov umožňujú proaktívny rámec pripravenosti a celkovej bezpečnosti a ochrany v prípade incidentov alebo kybernetických hrozieb.
- jednoduché rutinné opatrenia, ktoré minimalizujú vystavenie sa rizikám kybernetických hrozieb, ak ich občania, organizácie a podniky vykonávajú pravidelne (Akt o kybernetickej bezpečnosti)

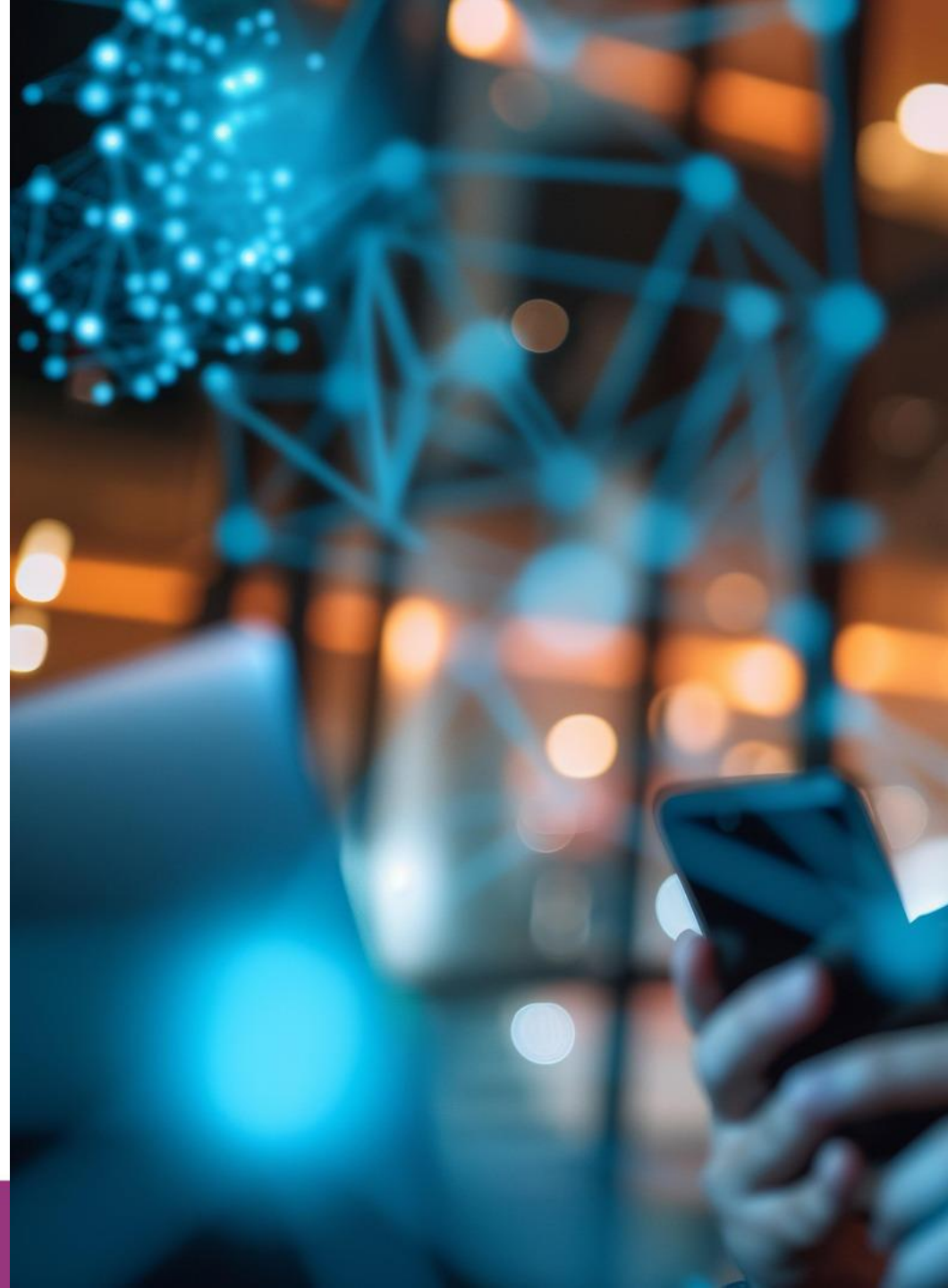
Opatrenia (čl. 21)

h) zásady a postupy používania kryptografie, prípadne šifrovania

i) bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív

j) v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu

Oznamovacie povinnosti



Kto?

Čo?

Komu?

Lehota?

Incidenty

Hrozby

Udalosti

Zraniteľnosti

Incidenty

Oznamovacie povinnosti (čl. 23)

- každý **incident so závažným vplyvom** na poskytovanie ich služieb (**významný incident**)
- **bez zbytočného odkladu**
- **jednotke CSIRT** alebo v náležitých prípadoch svojmu **príslušnému orgánu**

Oznamovacie povinnosti (čl. 23)

- **oznámiť príjemcom svojich služieb** významné 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

Incident

- **„incident“** je udalosť ohrozujúca **dostupnosť, pravosť, integritu alebo dôvernosť** uchovávaných, prenášaných alebo spracúvaných **údajov** alebo **služieb** poskytovaných alebo prístupných prostredníctvom **sietí a informačných systémov**;

- „**rozsiahly kybernetický incident**“ je incident, ktorý spôsobí **narušenie na úrovni presahujúcej schopnosť** členského štátu naň reagovať alebo ktorý má významný vplyv **aspoň na dva členské štáty**;

Oznamovacie povinnosti (čl. 23)

Vykonávacie akty

- **Incident sa považuje za významný, ak:**
  - spôsobil alebo má schopnosť spôsobiť dotknutému subjektu **závažné prevádzkové narušenie služieb alebo finančnú stratu**;
  - **zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby** tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu.

CUSEC

Oznamovacie povinnosti (čl. 23)

Druh	Lehota	Obsahové náležitosti (v prípade potreby)
včasné varovanie (early warning)	bez zbytočného odkladu najneskôr do **24** hodín od zistenia významného incidentu	• či významný incident pravdepodobne spôsobilo konanie, ktoré je nezákonné alebo so zlým úmyslom, alebo či môže mať cezhraničný dosah;
oznámenie o incidente	bez zbytočného odkladu najneskôr do **72** hodín od zistenia významného incidentu *poskytovateľ dôveryhodných služieb do 24 hodín	• aktualizovanie informácií z včasného varovania, • prvotné posúdenie významného incidentu, vrátane jeho závažnosti a vplyvu, ako aj prípadne indikátory kompromitácie.
priebežná správa s relevantnou aktualizáciou daného stavu	na základe požiadania jednotky CSIRT alebo v náležitých prípadoch príslušného orgánu	

Druh oznámenia	Lehota	Obsahové náležitosti
záverečná správa	najneskôr **jeden mesiac** po postúpení oznámenia o incidente	• podrobný opis incidentu vrátane jeho závažnosti a vplyvu; • druh hrozby alebo hlavnú príčinu, ktorá pravdepodobne incident spôsobila; • zavedené a prebiehajúce zmierňujúce opatrenia; • v náležitých prípadoch cezhraničný vplyv incidentu;
prebiehajúce incidenty **ďalšia priebežná správa (progress report)**	• v čase keď mali podať záverečnú správu • záverečnú správu do jedného mesiaca po vyriešení incidentu	

Povinnosti po oznámení (čl. 23)

- **Jednotka CSIRT/príslušný orgán**

Druh	Lehota	Poznámka
odpoveď oznamovateľovi	bez zbytočného odkladu a v rámci možností do 24 hodín od doručenia včasného varovania	• vrátane **prvotnej spätnej väzby** k významnému incidentu a na žiadosť subjektu usmernenie alebo operačné pokyny k vykonávaniu možných zmierňujúcich opatrení. • jednotka CSIRT poskytne **doplňujúcu technickú podporu**, ak o to dotknutý subjekt požiada. • ak existuje podozrenie, že **významný incident je trestnoprávnej povahy,** jednotka CSIRT alebo príslušný orgán poskytne aj usmernenie, ako významný incident oznámiť orgánom presadzovania práva.

Oznamovacie povinnosti (čl. 23)

- **2 a viac ČS**
- jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto
- bez zbytočného odkladu
- informovať **iné zasiahnuté** ČŠ + ENISA

Oznamovacie povinnosti (čl. 23)

- **informovanie verejnosti**
- jednotka CSIRT, prípadne príslušný orgán členského štátu
- po **porade** s dotknutým subjektom
- alebo **požiadať o to daný subjekt**
  - ak je informovanie verejnosti **potrebné na zabránenie významnému incidentu** alebo **riešenie prebiehajúceho incidentu**
  - alebo ak je zverejnenie významného incidentu **vo verejnom záujme** z iného dôvodu.

Hrozby

Hrozba

- „**kybernetická hrozba**“ je každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby (Akt o KB)

- „**významná kybernetická hrozba**“ je kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že **má potenciál mať závažný vplyv na sieť a informačné systémy subjektu alebo používateľov služieb subjektu** tým, že spôsobí značnú hmotnú alebo nehmotnú ujmu.

Oznamovacie povinnosti (čl. 23)

- **Významné kybernetické hrozby**

- Členské štáty v náležitých prípadoch zabezpečia, aby kľúčové a dôležité subjekty **bez zbytočného odkladu** oznámili **príjemcom svojich služieb**, ktorí potenciálne **čelia významnej kybernetickej hrozbe**, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať.

- Subjekty **v prípade potreby** týchto príjemcov informujú aj **o samotnej významnej kybernetickej hrozbe**.

Udalosti

Dobrovoľné oznámenie relevantných informácií (čl. 30)

udalosť odvrátená v poslednej chvíli

- udalosť, ktorá by **mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť** uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale **ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo**;

CUSEC

Dobrovoľné oznámenie relevantných informácií (čl. 30)

- Členské štáty zabezpečia, aby **okrem oznamovacej povinnosti** stanovenej v článku 23 mohli jednotkám CSIRT alebo prípadne príslušným orgánom **podávať oznámenia dobrovoľne** tieto subjekty:

  - kľúčové a dôležité subjekty **v súvislosti s incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli**;

  - **iné subjekty**, než sú subjekty uvedené v písmene a), bez ohľadu na to, či patria do rozsahu pôsobnosti tejto smernice, **v súvislosti s významnými incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli**.

Zraniteľnosti

Zraniteľnosti

- „**zraniteľnosť**“ je slabá stránka, náchylnosť alebo chyba produktov IKT alebo služieb IKT, ktorá **môže byť zneužitá kybernetickou hrozbou**;

- Členské štáty zabezpečia, aby **fyzické alebo právnické osoby** mohli na požiadanie nahlásiť zraniteľnosť **jednotke CSIRT** určenej za koordinátora anonymne.

CUSEC

Vykonávacie akty

- Vybraní poskytovatelia služieb (povinnosť prijať do 17.10.2024)
- Ostatné KS a DS (len možnosť)

CUSEC

Vykonávacie akty

- poskytovateľov služieb DNS,
- správcov názvov TLD,
- poskytovateľov služieb cloud computingu,
- poskytovateľov služieb dátového centra,
- poskytovateľov sietí na sprístupňovanie obsahu,
- poskytovateľov riadených služieb,
- poskytovateľov riadených bezpečnostných služieb,
- poskytovateľov online trhov,
- internetových vyhľadávačov,
- platforiem služieb sociálnej siete a
- poskytovateľov dôveryhodných služieb

Vykonávacie akty

- Vykonávacie nariadenie Komisie (EÚ) **2024/2690** zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o **technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík** a o bližšie určenie prípadov, v ktorých sa **incident považuje za významný**, vo vzťahu k **poskytovateľom** služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb

Vybraní poskytovatelia služieb

BO na riadenie kybernetických rizík

Významný incident

CUSEC

Vykonávacie nariadenie 2024/2690

BO na riadenie kybernetických rizík

- Príloha

- Technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík uvedené v článku 21 ods. 2 písm. a) až j)

CUSEC

Riešenie incidentov [článok 21 ods. 2 písm. b)]

BO na riadenie kybernetických rizík

- príslušné subjekty **stanovia a vykonávajú zásady riešenia incidentov**, ktorými sa stanovujú **úlohy, povinnosti a postupy** na:
  - včasné odhaľovanie incidentov,
  - ich analýzu,
  - zamedzenie ich šíreniu alebo
  - reagovanie na ne,
  - zotavenie sa z nich,
  - ich zaznamenávanie a oznamovanie.

CUSEC

Vykonávacie nariadenie 2024/2690

Významný incident

- ak je splnené **aspoň jedno z týchto kritérií**:

a) incident príslušnému subjektu spôsobil alebo môže spôsobiť priamu **finančnú stratu, ktorá prevyšuje 500 000 EUR alebo 5 % celkového ročného obratu** príslušného subjektu za predchádzajúci finančný rok, podľa toho, ktorá suma je nižšia;

b) incident spôsobil alebo môže spôsobiť **únik obchodných tajomstiev** príslušného subjektu, ako sú vymedzené v článku 2 bode 1 smernice (EÚ) 2016/943;

c) incident spôsobil alebo môže spôsobiť **smrť fyzickej osoby**;

CUSEC

Vykonávacie nariadenie 2024/2690

Významný incident

d) incident spôsobil alebo môže spôsobiť **značné poškodenie zdravia fyzickej osoby**;

e) došlo k **úspešnému**, domnelo zlomyseľnému a **neoprávnenému prístupu do sietí a informačných systémov**, ktorý by mohol spôsobiť **vážne narušenie prevádzky**;

f) incident spĺňa kritériá uvedené v článku 4; (**opakujúce sa incidenty**)

g) incident spĺňa aspoň jedno z kritérií uvedených v článkoch 5 až 14. (**výzmanmý incident príslušného subjketu**)

Vykonávacie nariadenie 2024/2690

Pri **výpočte počtu používateľov** dotknutých incidentom (na účely článku 7 a článkov 9 až 14) príslušné subjekty zohľadnia všetky tieto údaje:

1. **počet zákazníkov**, ktorí **uzatvorili zmluvu** s príslušným subjektom, ktorý im poskytuje prístup k svojim sieťam a informačným systémom alebo k službám poskytovaným alebo prístupným prostredníctvom týchto sietí a informačných systémov;

2. **počet fyzických a právnických osôb** spojených **s komerčnými zákazníkmi**, ktorí **používajú siete a informačné systémy alebo služby** poskytované alebo prístupné prostredníctvom týchto sietí a informačných systémov.

CUSEC

Poskytovatelia platforiem služieb sociálnej siete

Významný incident

- platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, najmä prostredníctvom chatov, príspevkov, videí a odporúčaní (NIS 2)

- ak spĺňa **aspoň jedno z kritérií**

Poskytovatelia platforiem služieb sociálnej siete

- platforma služieb sociálnej siete je **úplne nedostupná** **pre viac ako 5 % používateľov** tejto platformy služieb sociálnej siete v Únii **alebo pre viac ako 1 milión používateľov** tejto platformy služieb sociálnej siete v Únii, podľa toho, **ktorý údaj je nižší**;

- **viac ako 5 % používateľov** platformy služieb sociálnej siete v Únii alebo viac ako **1 milión používateľov** platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je **nižší**, je **dotknutých** **obmedzenou dostupnosťou** tejto platformy služieb sociálnej siete;

Poskytovatelia platforiem služieb sociálnej siete

- **integrita, dôvernosť alebo pravosť** uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním platformy služieb sociálnej siete je **ohrozená** v dôsledku domnelo **zlomyseľného konania**;

- **integrita, dôvernosť alebo pravosť** uchovávaných, prenášaných alebo spracúvaných údajov súvisiacich s poskytovaním platformy služieb sociálnej siete je **ohrozená s dosahom** na viac ako **5 % používateľov** tejto platformy služieb sociálnej siete v Únii alebo na viac ako **1 milión používateľov** tejto platformy služieb sociálnej siete v Únii, podľa toho, ktorý údaj je nižší.

Dohľad a presadzovanie práva

Dohľad a presadzovanie práva

- **Čl. 32 – kľúčové subjekty**
- plnohodnotný režim dohľadu (ex ante a ex post)

- **Čl. 33 – 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 (KS)

- **príslušné orgány** pri vykonávaní svojich úloh **dohľadu** nad kľúčovými subjektmi mali **právomoc podrobiť** tieto subjekty prinajmenšom:
  - inšpekciám na mieste a dohľadu na diaľku
  - pravidelným a cieleným bezpečnostným auditom
  - auditom ad hoc
  - bezpečnostným kontrolám
  - žiadostiam o informácie
  - žiadostiam o prístup k údajom
  - žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti

Dohľad a presadzovanie práva (KS)

- **príslušné orgány** pri vykonávaní svojich **právomocí presadzovania práva** v súvislosti s kľúčovými subjektmi mali **právomoc** prinajmenšom:
  - vydávať **varovania** o porušeniach tejto smernice dotknutými subjektmi;
  - prijímať **záväzné pokyny** alebo **príkaz**, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenia tejto smernice;
  - **nariadiť** dotknutým subjektom, aby **upustili od konania**, ktoré porušuje túto smernicu, a takéto konanie neopakovali;
  - nariadiť dotknutým subjektom, aby **určeným spôsobom a v určenej lehote zosúladili svoje opatrenia** na riadenie kybernetických rizík s článkom 21 alebo **splnili oznamovacie povinnosti** stanovené v článku 23;

Dohľad a presadzovanie práva (KS)

- nariadiť dotknutým subjektom, aby **informovali** fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté **významnou kybernetickou hrozbou**, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na danú hrozbu;

- nariadiť dotknutým subjektom, aby v primeranej lehote **vykonali odporúčania** poskytnuté na základe bezpečnostného auditu;

- určiť **monitorujúceho úradníka** s presne vymedzenými úlohami na určité obdobie, ktorý bude dohliadať na dodržiavanie článkov 21 a 23 dotknutými subjektmi;

Dohľad a presadzovanie práva (KS)

- nariadiť dotknutým subjektom, aby určeným spôsobom **zverejnili** aspekty **porušovania** tejto smernice;

- **uložiť správnu pokutu** podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až h) tohto odseku.

CUSEC

Dohľad a presadzovanie práva (KS)

- opatrenia na presadzovanie práva **neúčinné**?

- príslušné orgány stanovia **lehotu**, v rámci ktorej je kľúčový subjekt povinný prijať potrebné opatrenia na nápravu nedostatkov alebo splniť požiadavky týchto orgánov.

- opatrenia sa v **lehote neprijali**?

CUSEC

Dohľad a presadzovanie práva (KS)

Príslušné orgány:

- **dočasne** pozastaviť **certifikáciu** alebo **povoľovanie** alebo **požiadať** certifikačný alebo povoľujúci subjekt, súd, alebo tribunál v súlade s vnútroštátnym právom, **aby dočasne pozastavil certifikáciu alebo povoľovanie časti alebo všetkých relevantných služieb**, ktoré kľúčový subjekt **poskytuje**, alebo činností, ktoré kľúčový subjekt vykonáva;

- od **príslušných orgánov, súdov alebo tribunálov** v súlade s vnútroštátnym právom požadovať **uloženie** dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to **akejkoľvek fyzickej osobe** zodpovednej za vykonávanie **riadiacich úloh** na úrovni **výkonného riaditeľa alebo právneho zástupcu** v tomto kľúčovom subjekte.

Správne pokuty

kľúčovým subjektom v prípade porušenia článku 21 alebo 23 boli

- **v maximálnej výške aspoň 10 000 000 EUR alebo v maximálnej výške aspoň 2 % celkového celosvetového ročného obratu** v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia.

dôležitým subjektom v prípade porušenia článku 21 alebo 23

- **v maximálnej výške aspoň 7 000 000 EUR alebo v maximálnej výške aspoň 1,4 % celkového celosvetového ročného obratu** v predchádzajúcom finančnom roku podniku, ku ktorému dôležitý subjekt patrí, podľa toho, ktorá suma je vyššia.

- možnosť stanoviť aj pravidelné penále

Akt o kybernetickej bezpečnosti

Akt o kybernetickej bezpečnosti

- nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o **agentúre ENISA (Agentúre Európskej únie pre kybernetickú bezpečnosť)** a o **certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií** a o zrušení nariadenia (EÚ) č. 526/2013 („akt o kybernetickej bezpečnosti").

- zaistiť riadne fungovanie vnútorného trhu,
- usiluje o dosiahnutie vysokej úrovne kybernetickej bezpečnosti, kybernetickej **odolnosti** a **dôvery** v rámci EÚ.

Akt o kybernetickej bezpečnosti

- definovali ciele, úlohy a organizačné aspekty týkajúce sa **agentúry ENISA** (**Agentúra Európskej únie pre kybernetickú bezpečnosť**)

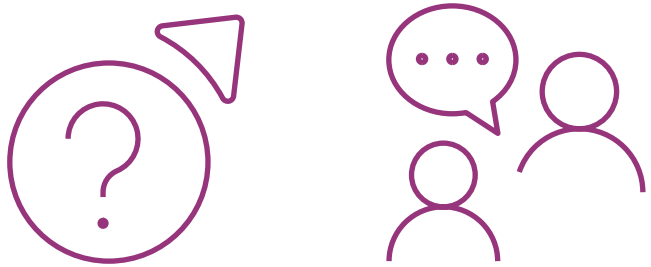
enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY
20 years!

CUSEC

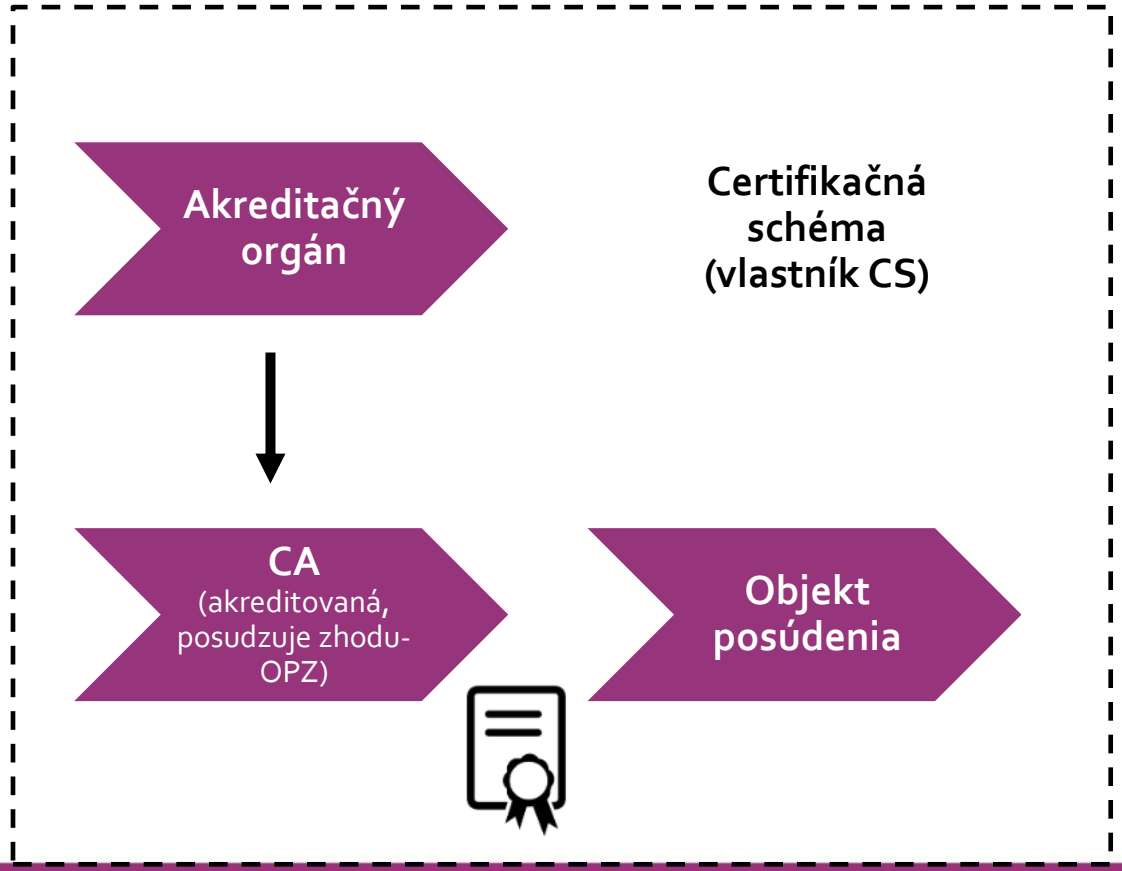
Akt o kybernetickej bezpečnosti

- vytvára rámec pre zavádzanie **európskych systémov certifikácie kybernetickej bezpečnosti** na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v EÚ.

Čo je certifikácia?



Akt o kybernetickej bezpečnosti



Akt o kybernetickej bezpečnosti

CUSEC

CA - akreditovaná ,vnútroštátny orgán, nezávislý, PS

- **Európsky systém certifikácie kybernetickej bezpečnosti**
- **vytvára rámec pre prijímanie** európskych certifikačných schém
  - produkty IKT (napr. router),
  - služby IKT (napr. autentifikácia klientov online) a
  - procesy IKT (napr. systém riadenia bezpečnosti informácií).

- **európsky certifikát kybernetickej bezpečnosti**
  - uznávaný vo všetkých ČŠ

Akt o kybernetickej bezpečnosti

- **Európsky systém certifikácie kybernetickej bezpečnosti (ciele)**

a) *chrániť uchovávané, prenášané alebo inak spracúvané údaje pred **náhodným či neoprávneným uchovávaním, spracúvaním, prístupom alebo poskytnutím** počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;*

b) *chrániť uchovávané, prenášané alebo inak spracúvané údaje **pred náhodným či neoprávneným zničením, stratou alebo zmenou alebo nedostatočnou dostupnosťou** počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;*

c) *umožňovať **oprávneným** osobám, programom alebo zariadeniam **prístup** výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;*

d) *identifikovať a dokumentovať známe závislosti a zraniteľnosti;*

e) *zaznamenávať, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;*

Akt o kybernetickej bezpečnosti

- **Európsky systém certifikácie kybernetickej bezpečnosti**

f) *umožňovať overenie, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;*

g) *overovať, či produkty IKT, služby IKT a procesy IKT neobsahujú známe zraniteľnosti;*

h) *v prípade fyzického alebo technického incidentu včas* ***obnoviť dostupnosť údajov, služieb a funkcií a prístup k nim****;*

i) *aby produkty IKT, služby IKT a procesy IKT boli bezpečné štandardne a* ***už v štádiu návrhu****;*

j) *aby sa produkty IKT, služby IKT a procesy IKT dodávali alebo poskytovali s* ***aktualizovaným softvérom a hardvérom****, ktoré neobsahujú verejne známe zraniteľnosti, a dodávali alebo poskytovali s mechanizmami na bezpečnú aktualizáciu.*

Akt o kybernetickej bezpečnosti

- **Úrovne záruky (*assurance level*)**
  - **základná,**
  - **pokročilá** a
  - **vysoká** (OPZ – verejný subjekt)
- každý európsky certifikát kybernetickej bezpečnosti bude uvádzať jede z troch úrovní záruky
- **vlastné posúdenie zhody** (základná ÚZ – nízke riziko z hľadiska verejného záujmu)

Akt o kybernetickej bezpečnosti

- **Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskeho systému certifikácie kybernetickej bezpečnosti založeného na spoločných kritériách (EUCC)**

PRESS RELEASE

An EU Prime! EU adopts first Cybersecurity Certification Scheme

The European Cybersecurity Scheme on Common Criteria (EUCC) drafted by the European Union Agency for Cybersecurity (ENISA) has been adopted as the first scheme within the EU cybersecurity certification framework.

Published on January 31, 2024

Akt o kybernetickej bezpečnosti

- v súlade s európskym rámcom certifikácie kybernetickej bezpečnosti stanoveným
- špecifikujú úlohy, pravidlá a povinnosti, ako aj štruktúra **európskeho systému certifikácie kybernetickej bezpečnosti založeného na spoločných kritériách** (ďalej len „**EUCC**")
- Systém by mal vychádzať zo zavedených medzinárodných noriem.
  - ISO/IEC 15408 - Information security, cybersecurity and privacy protection Evaluation criteria for IT security Part 1: Introduction and general model.
  - ISO/IEC 18045 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation

Akt o kybernetickej odolnosti

Akt o kybernetickej odolnosti

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)

- **Produkt s digitálnymi prvkami**
  - **hardvérové produkty** (napr. zariadenia internetu vecí – IoT, inteligentné domáce spotrebiče, priemyselné riadiace systémy, mikročipy),
  - **softvérové produkty** (napr. videohry, aplikácie, počítačové programy).

Akt o kybernetickej odolnosti

- **Ohlasovacie povinnosti výrobcov**
  - bez zbytočného odkladu oznámiť
    - závažné kybernetickobezpečnostné incidenty a
    - aktívne zneužívané zraniteľnosti príslušným vnútroštátnym orgánom a ENISA
  - informovať používateľov o potenciálnych rizikách a poskytovať im usmernenia na ich zmiernenie.

Ďakujem za pozornosť!