KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Úvod do právnej úpravy kybernetickej bezpečnosti

Meno a priezvisko

XX.XX.XXXX

KCKB UPJS CSIRT UPJS

Svet okolo nás (I.)

2024

22.3.2024 15:46 | Bezpečnosť

Hackeri udreli na Slovenskú národnú knižnicu. Nejdú prístupy k zdrojom ani kontakty

Zdroj: reprofoto Snk.sk, iStock a úprava redakcia

Rumunské nemocnice napadnuté ransomvérom

Vypublikované 13. 02. 2024

ransomware-nemocnice-860x360

Najmenej 25 rumunských nemocníc bolo odrezaných od online služieb po tom, čo útok ransomvéru znefunkčnil ich systém na správu zdravotnej starostlivosti. Cieľom útoku bol HIS, ktorý sa používa v nemocniciach na správu lekárskej činnosti a údajov o pacientoch. Útok, ktorý sa odohral počas noci z 11. na 12. februára 2024, zasiahol produkčné servery HIS a v dôsledku toho s**ystém prestal fungovať**, súbory a databázy boli zašifrované. **Rumunské ministerstvo zdravotníctva** uviedlo, že incident je predmetom vyšetrovania IT špecialistami, vrátane odborníkov na kybernetickú bezpečnosť z Národného riaditeľstva pre kybernetickú bezpečnosť (DNSC), a posudzujú sa možnosti obnovy. Zoznam zasiahnutých nemocníc bol aktualizovaný po zverejnení aktualizácie DNSC a zahŕňa nemocnice v rôznych regiónoch Rumunska vrátane centier pre regionálnu a onkologickú liečbu.

Zdroj: https://www.nbu.gov.sk/rumunske-nemocnice-napadnute-ransomverom/, https://zive.aktuality.sk/clanok/1CGRx85/hackeri-udreli-na-slovensku-narodnu-kniznicu-nejdu-pristupy-k-zdrojom-ani-kontakty/

Svet okolo nás (II.)

2025

živé

Predplatné

TOP Kataster po mesiaci: Štát prelomil mlčanie. Čo radí a sľubuje ľuďom

Zdroj: iStock, reprofoto Zbgis.skgeodesy.sk, úprava redakcia

Lukáš Kosno

Filip Hanker

Zhrnuli sme novinky okolo katastra presne mesiac po útoku. Máme oficiálne vyjadrenia úradu.

TREND

Predplatiť

Hekeri po útoku na kataster žiadajú vysoké výkupné, štát nemusí disponovať zálohami dát

Zdroj: Shutterstock

Daniel Ivančák
online editor

9.1. 7:35 | **Ak sa hekerský útok v takomto rozsahu potvrdí, na Slovensku môže nastať chaos**

Zdroj: https://www.nbu.gov.sk/rumunske-nemocnice-napadnute-ransomverom/, https://zive.aktuality.sk/clanok/1CGRx85/hackeri-udreli-na-slovensku-narodnu-kniznicu-nejdu-pristupy-k-zdrojom-ani-kontakty/


Neexistuje 100% bezpečnosť

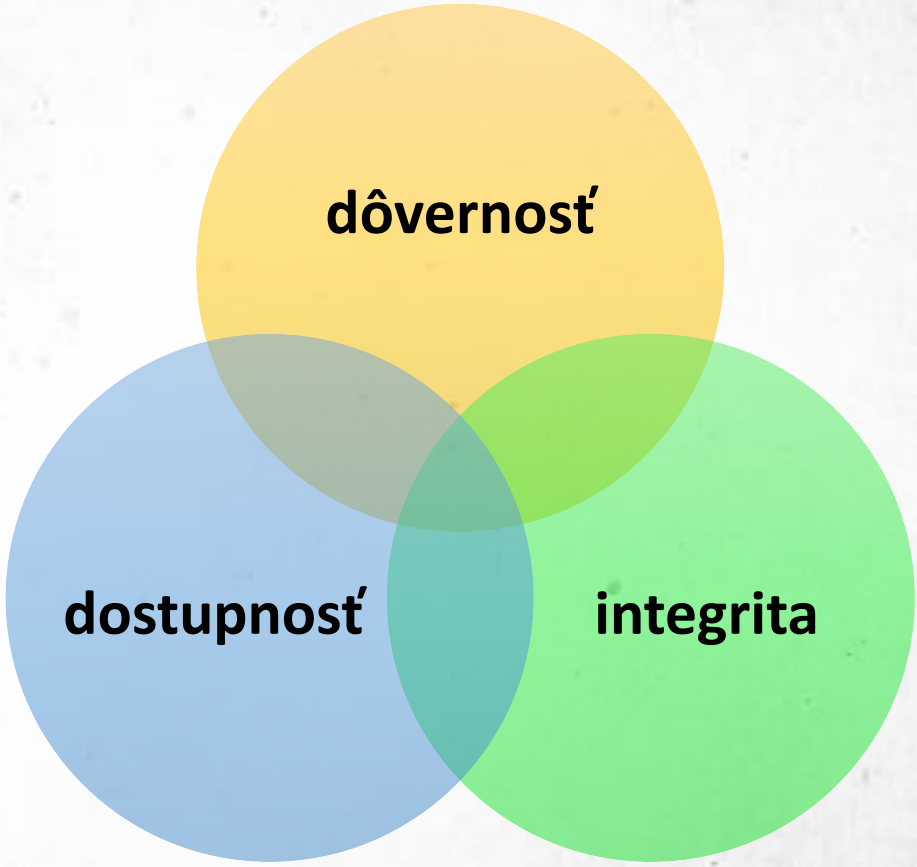
Čo je kybernetická bezpečnosť?

stav, v ktorom sú siete a informačné systémy ***schopné odolávať na určitom stupni*** *spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje* ***dostupnosť, pravosť, integritu alebo dôvernosť*** *uchovávaných, prenášaných alebo spracúvaných* ***údajov*** *alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov*

(§ 3 ods. 1 písm. h) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ZoKB))

Kybernetická bezpečnosť (II.)

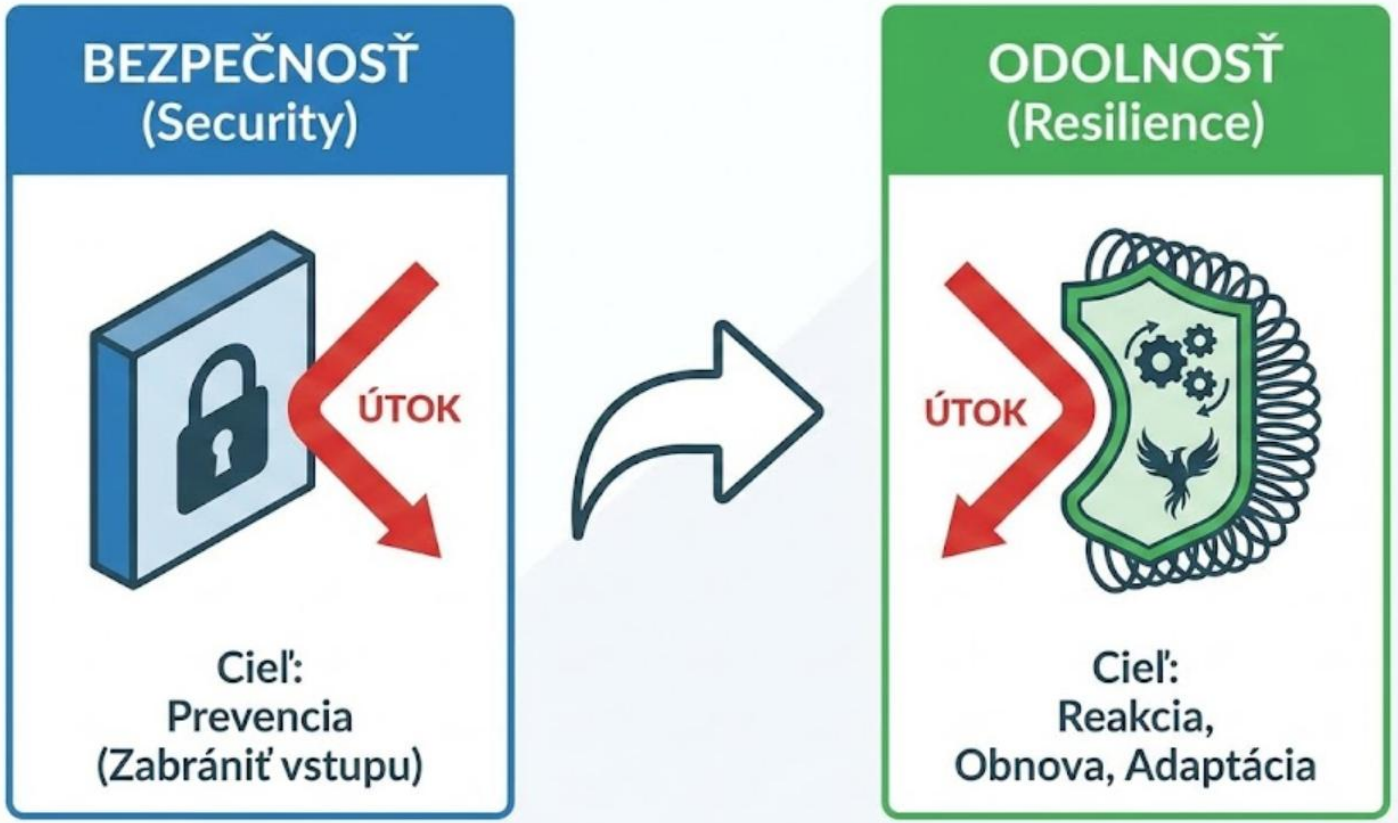
- **dôvernosť**
  - záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom (§3 ods. 1 písm. e) ZoKB)
- **integrita**
  - záruka, že bezchybnosť, úplnosť alebo správnosť údaja neboli narušené (§3 ods. 1 písm. g) ZoKB)
- **Dostupnosť**
  - záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované (§3 ods. 1 písm. f) ZoKB)



ODOLNOSŤ VOČI KYBERNETICKÝM HROZBÁM

„Skutočná odolnosť nespočíva v tom, že zabránime každému útoku, ale v tom, ako rýchlo a efektívne sa dokážeme zotaviť.“

Kybernetická hrozba (II.)



Zdroj: Vygenerované pomocou AI Google Gemini

Kybernetická hrozba (III.)

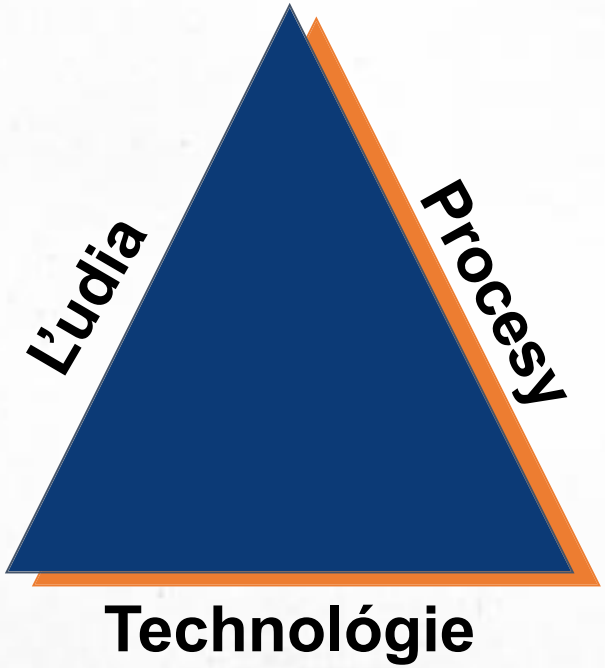
- **kybernetická hrozba**
  - je **každá potenciálna okolnosť**, **udalosť alebo činnosť**, ktorá by mohla poškodiť, narušiť alebo inak **negatívne ovplyvniť** siete a informačné systémy, užívateľov takýchto systémov a iné osoby (§ 3 ods. 1 písm. j) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti – odkazuje sa na Nariadenie 2019/881 (akt o kybernetickej bezpečnosti))

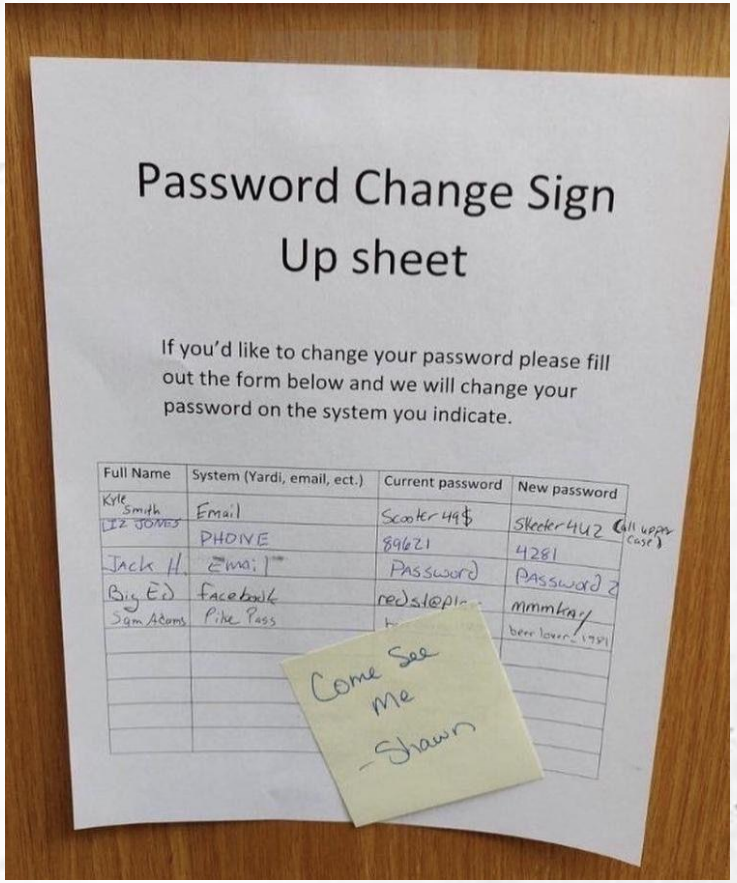
Zdroj: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Kybernetická bezpečnosť (I.)

- **kybernetická bezpečnosť**
  - **sú činnosti** potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami (článok 2 ods. 1 Nariadenia 2019/881 (akt o kybernetickej bezpečnosti))

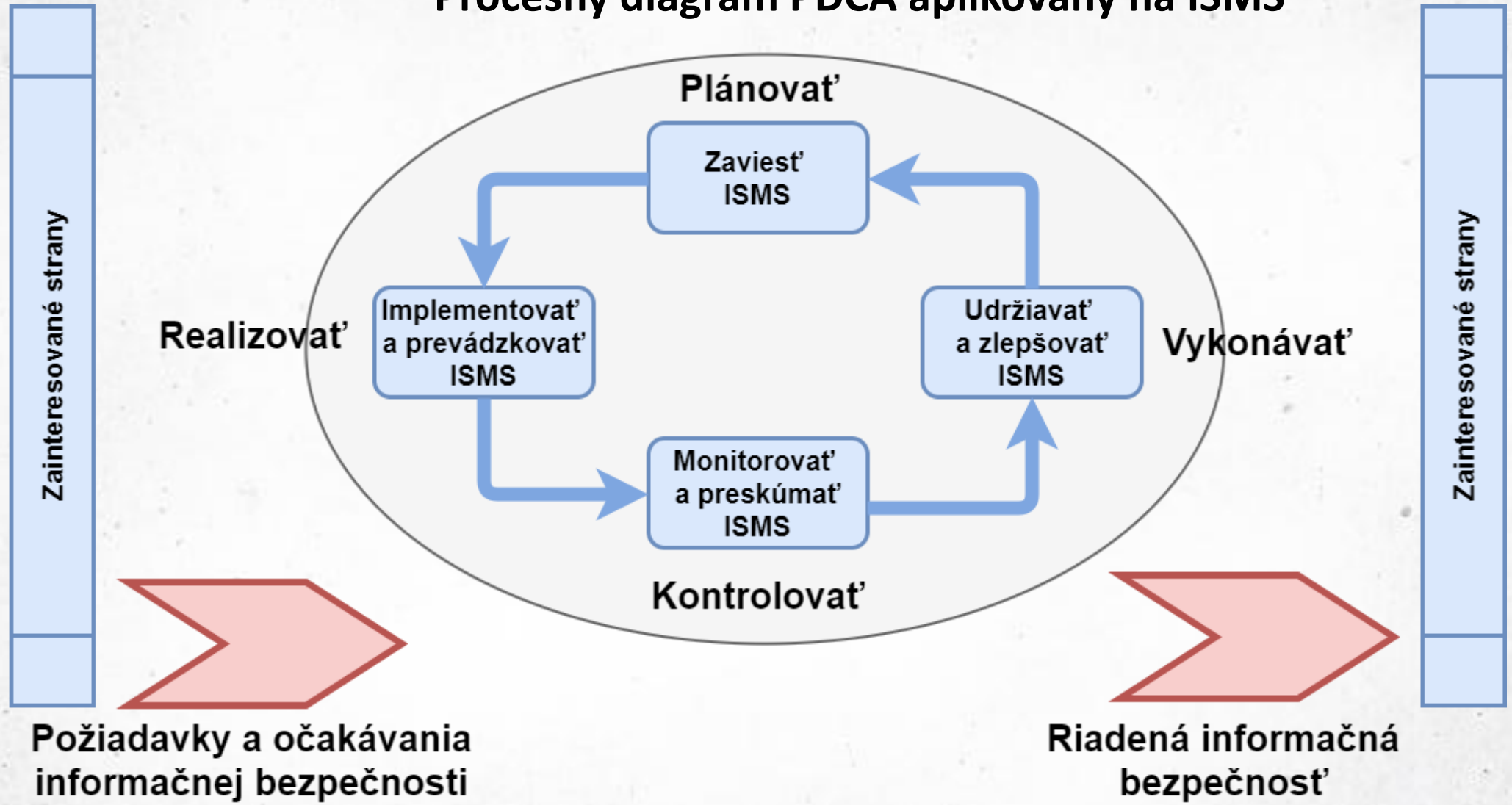
- kybernetická bezpečnosť je neustály proces, nie stav
- ide o prepojenie procesov, ľudí a technológií





Kybernetická bezpečnosť (II.)

Procesný diagram PDCA aplikovaný na ISMS



Princípy právnej úpravy KB (I.)

- Polčák, R. (2015). Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie*, *6*(11), 95-149.

1. Princíp technologickej neutrality

- všeobecný princíp pre oblasť IT práva
- právna regulácia je oddelená od konkrétnych technológií a spôsobov prenosu či ukladania informácií;
- IT/OT/AI sú neutrálne z hľadiska ich použitia.
- právny rámec nepreferuje ani nevylučuje konkrétnych dodávateľov alebo produkty a je nezávislý od technologického riešenia.

2. Princíp ochrany informačného sebaurčenia človeka

- zahŕňa ochranu základných informačných práv, najmä práva na súkromie a ochranu osobných údajov.
- súčasťou je aj právo na prístup k informáciám a službám informačnej spoločnosti, ktoré sú nevyhnutné pre plnohodnotný život v digitálnej spoločnosti.

Princípy právnej úpravy KB (II.)

3. Princíp ochrany nedistributívnych práv

- zameriava sa najmä na ochranu národnej bezpečnosti a bezpečnosti informačného prostredia ako celku.
- ide o ochranu prostredia, v ktorom prebiehajú informačné transakcie, a ktoré má charakter verejného statku.
- kybernetickú bezpečnosť je chápaná ako predpoklad fungovania vnútorného trhu a spoločnosti ako celku – bezpečné digitálne prostredie je verejný statok
- povinnosti sú viazané na subjekty zabezpečujúce základné služby

4. Princíp minimalizácie štátneho donútenia

- zásahy štátu do práv a slobôd sú prípustné len v nevyhnutne potrebnom rozsahu v súlade s testom proporcionality.
- rozlišuje sa medzi „essential“ a „important entities“ a existuje odstupňovaný dohľad

Princípy právnej úpravy KB (III.)

5. Princíp autonómie vôle regulovaných subjektov (princíp „výsledkovej“ regulácie)

- právna regulácia stanovuje cieľový stav, nie konkrétne technické alebo organizačné riešenia.
- regulované subjekty majú slobodu zvoliť si vlastné postupy na dosiahnutie požadovanej úrovne kybernetickej bezpečnosti.
- risk-based prístup

6. Princíp bdelosti vo vzťahu k iným štátom a medzinárodnému spoločenstvu (due diligence)

- štát nesie zodpovednosť za kybernetické bezpečnostné incidenty, ktoré vzniknú na jeho území alebo pod jeho jurisdikciou.
- princíp vyžaduje aktívne preventívne opatrenia a spoluprácu v rámci medzinárodného spoločenstva.

Európska právna úprava KB (I.)

- kybernetická bezpečnosť je tak vnímaná ako súčasť efektívneho fungovania vnútorného trhu EÚ.
- *„...siete a informačné systémy zohrávajú dôležitú úlohu pri uľahčovaní cezhraničného pohybu tovaru, služieb a osôb. Často sú navzájom prepojené a internet má globálny charakter. Vzhľadom na tento skutočne nadnárodný rozmer, narušenie v jednom členskom štáte môže mať vplyv aj na ďalšie členské štáty a EÚ ako celok. Preto je pre riadne fungovanie vnútorného trhu nevyhnutná odolnosť a stabilita sietí a informačných systémov.“ (Smernica NIS)*

Zdroj: https://secureframe.com/blog/eu-cybersecurity

Európska právna úprava KB (II.)

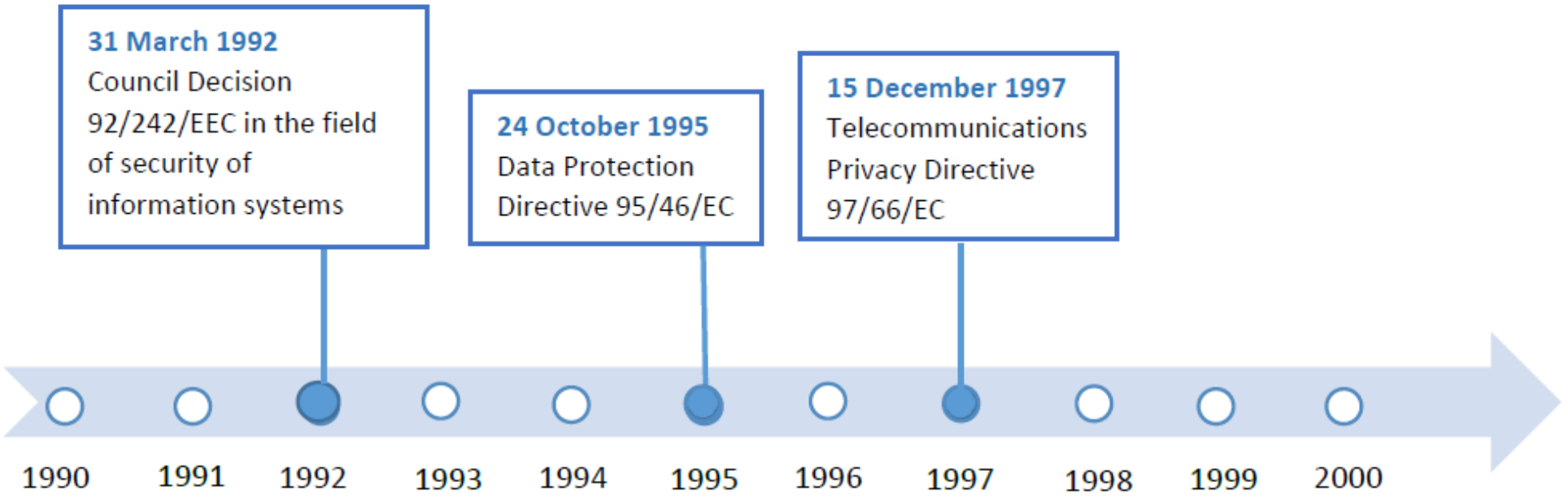


Figure 1: Legislative enactments 1990–2000

Zdroj: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4714393

Európska právna úprava KB (III.)

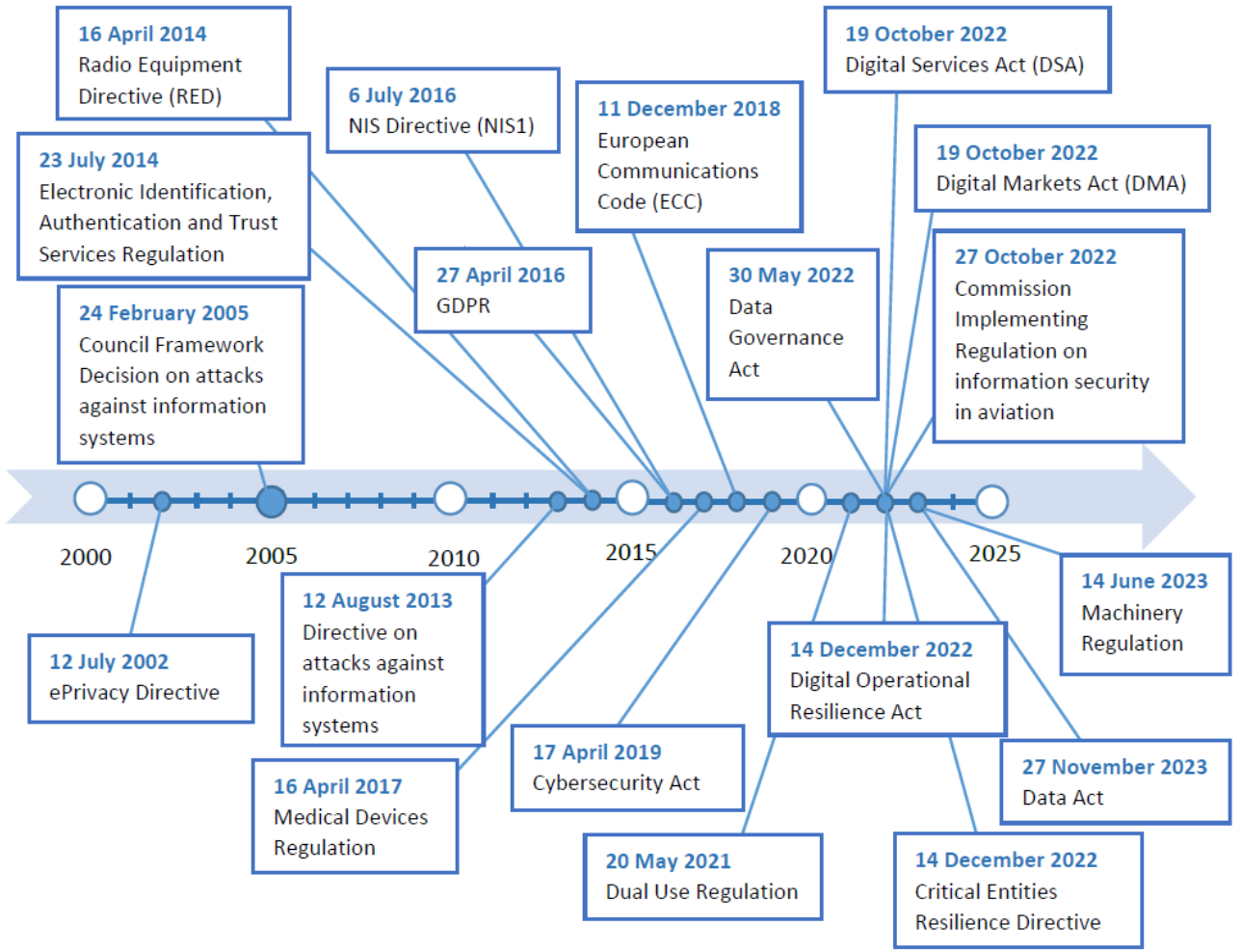
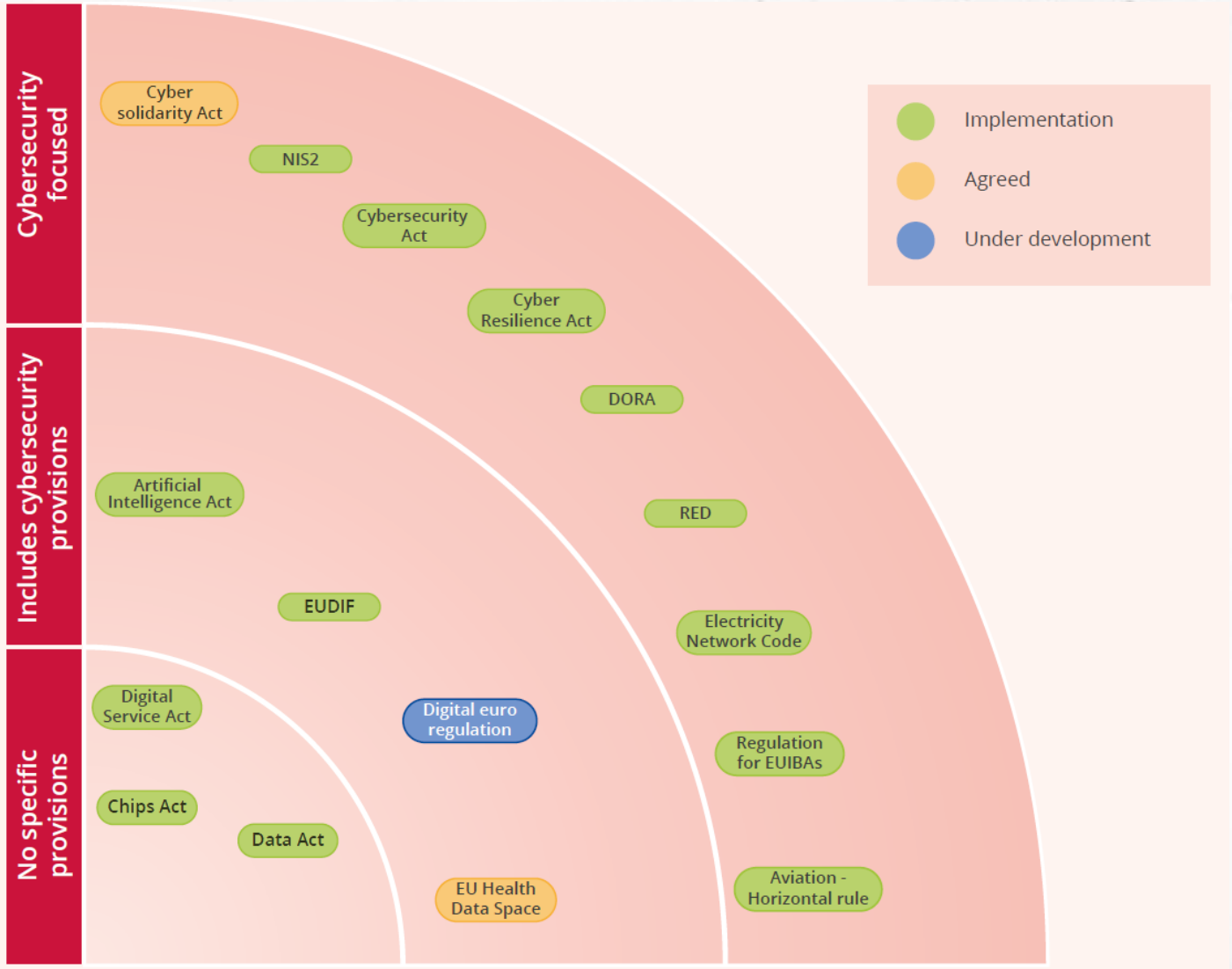


Figure 2: Legislative enactments 2000–2023

Zdroj: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4714393

Európska právna úprava KB (IV.)

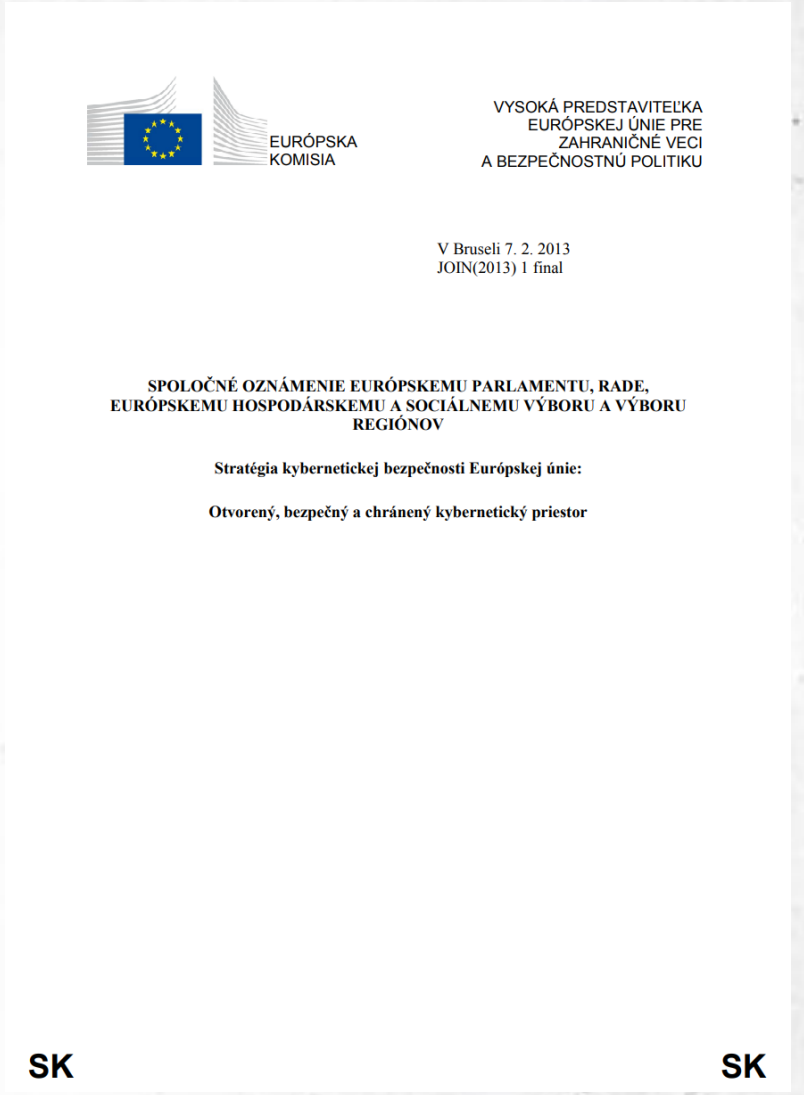


Zdroj: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

Stratégia kybernetickej bezpečnosti

Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor (2013)

- EÚ by mala chrániť online prostredie a pritom poskytovať všetkým najvyššiu možnú slobodu a bezpečnosť.
- riešenie bezpečnostných výziev v kybernetickom priestore je predovšetkým úlohou členských štátov
- stratégia navrhuje konkrétne opatrenia, ktoré môžu prispieť k zvýšeniu celkovej výkonnosti EÚ
- 5 strategických priorít:
  - dosiahnutie kybernetickej odolnosti
  - radikálne zníženie kybernetickej kriminality
  - rozvoj politiky a spôsobilostí kybernetickej obrany v súvislosti so spoločnou bezpečnostnou a obrannou politikou (SBOP)
  - rozvoj priemyselných a technologických zdrojov pre kybernetickú bezpečnosť
  - vytvorenie koherentnej medzinárodnej politiky kybernetického priestoru Európskej únie a podpora kľúčových hodnôt EÚ



EURÓPSKA KOMISIA

VYSOKÁ PREDSTAVITEĽKA EURÓPSKEJ ÚNIE PRE ZAHRANIČNÉ VECI A BEZPEČNOSTNÚ POLITIKU

V Bruseli 7. 2. 2013
JOIN(2013) 1 final

SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

Stratégia kybernetickej bezpečnosti Európskej únie:

Otvorený, bezpečný a chránený kybernetický priestor

SK SK

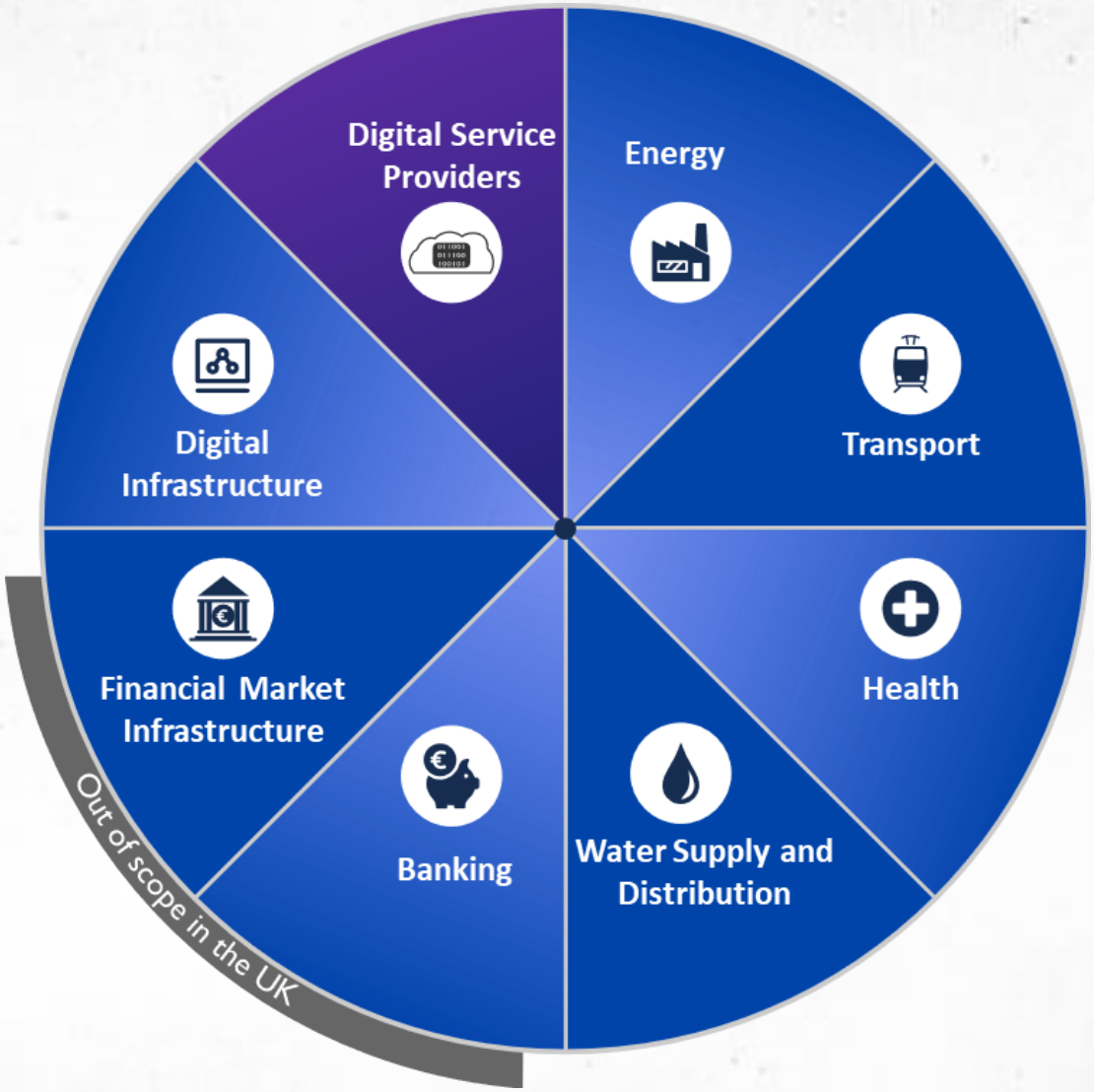
Smernica NIS (I.)

- **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**
- https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32016L1148

- prvý komplexný rámec EÚ pre kybernetickú bezpečnosť (2016)
- zaviedla povinnosti pre prevádzkovateľov základných služieb a digitálnych služieb
- ustanovila CSIRT tímy a mechanizmy spolupráce medzi členskými štátmi

- cieľom bolo budovať kapacity v oblasti kybernetickej bezpečnosti v celej Únii,
- zmierňovať hrozby pre siete a informačné systémy používané na poskytovanie základných služieb v kľúčových odvetviach a zabezpečiť kontinuitu takýchto služieb pri riešení incidentov, a tým prispievať k bezpečnosti Únie a účinnému fungovaniu jej hospodárstva a spoločnosti.

Smernica NIS (II.)



Zdroj: https://cetome.com/research/nis-directive/introduction

Smernica NIS2 (I.)

- **Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555** o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, mení a dopĺňa nariadenie (EÚ) č. 910/2014 a smernicu (EÚ) 2018/1972, a zrušuje smernicu (EÚ) 2016/1148 (smernica NIS)
- https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=sk

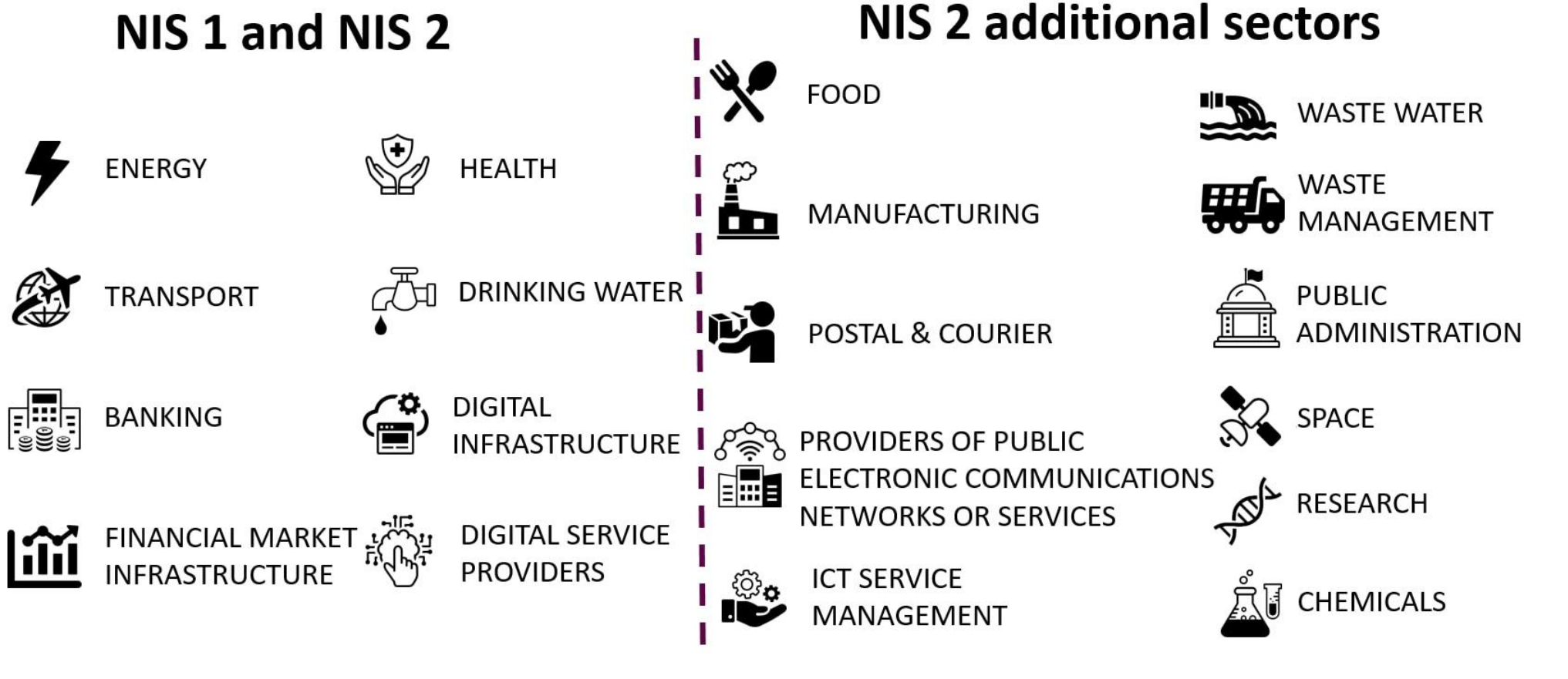
- Povinnosti v oblasti:
  - riadenia rizík
  - hlásenia incidentov
  - zodpovednosti manažmentu
- posilnenie CSIRT a orgánov dohľadu
- inštitucionalizácia siete **EU-CyCLONe**
- posilnená spolupráca medzi členskými štátmi

- posun od diskrečnej harmonizácie k záväzným minimám

- **NIS 1 = reaktívna regulácia**
- **NIS 2 = preventívno-riadiaci rámec**

Smernica NIS2 (II.)

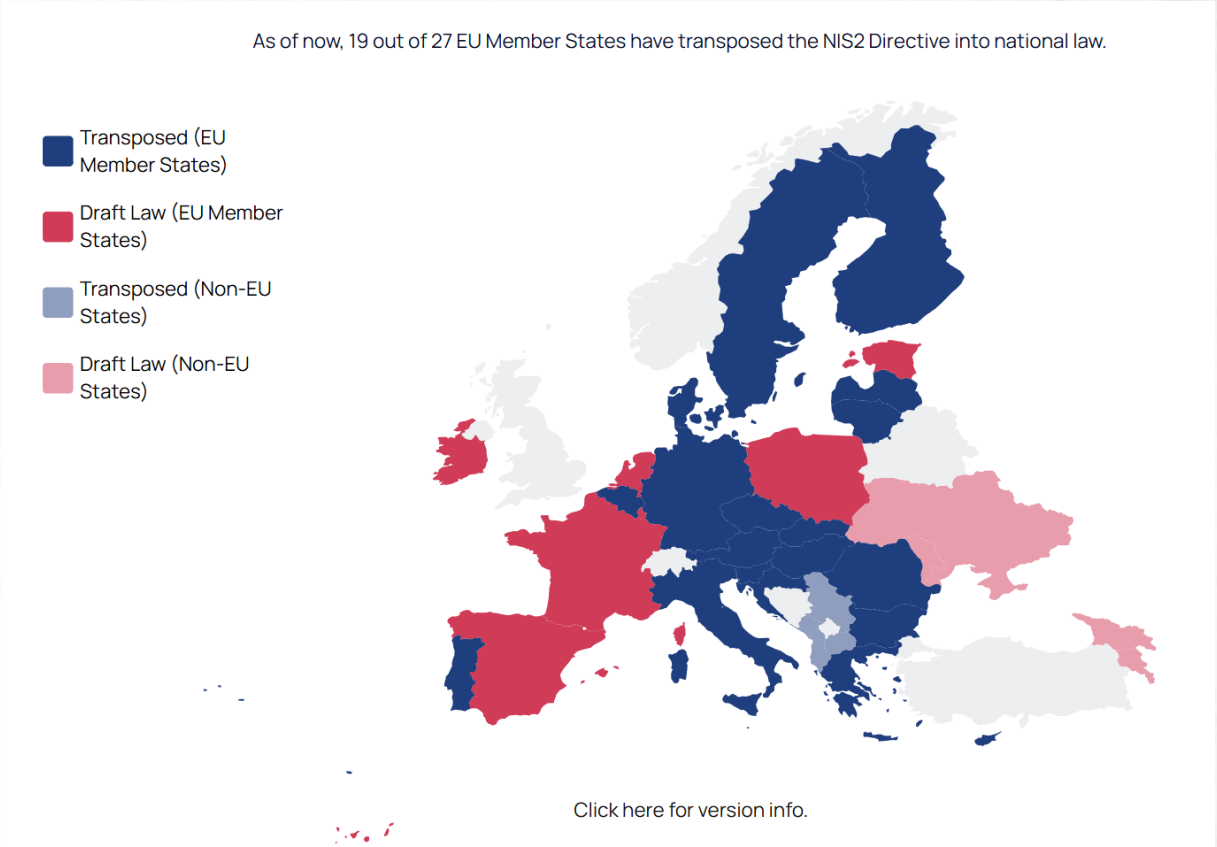
- výrazné rozšírenie pôsobnosti (18 sektorov)



Zdroj: https://www.fieldfisher.com/en-be/locations/belgium/insights/nis2-directive

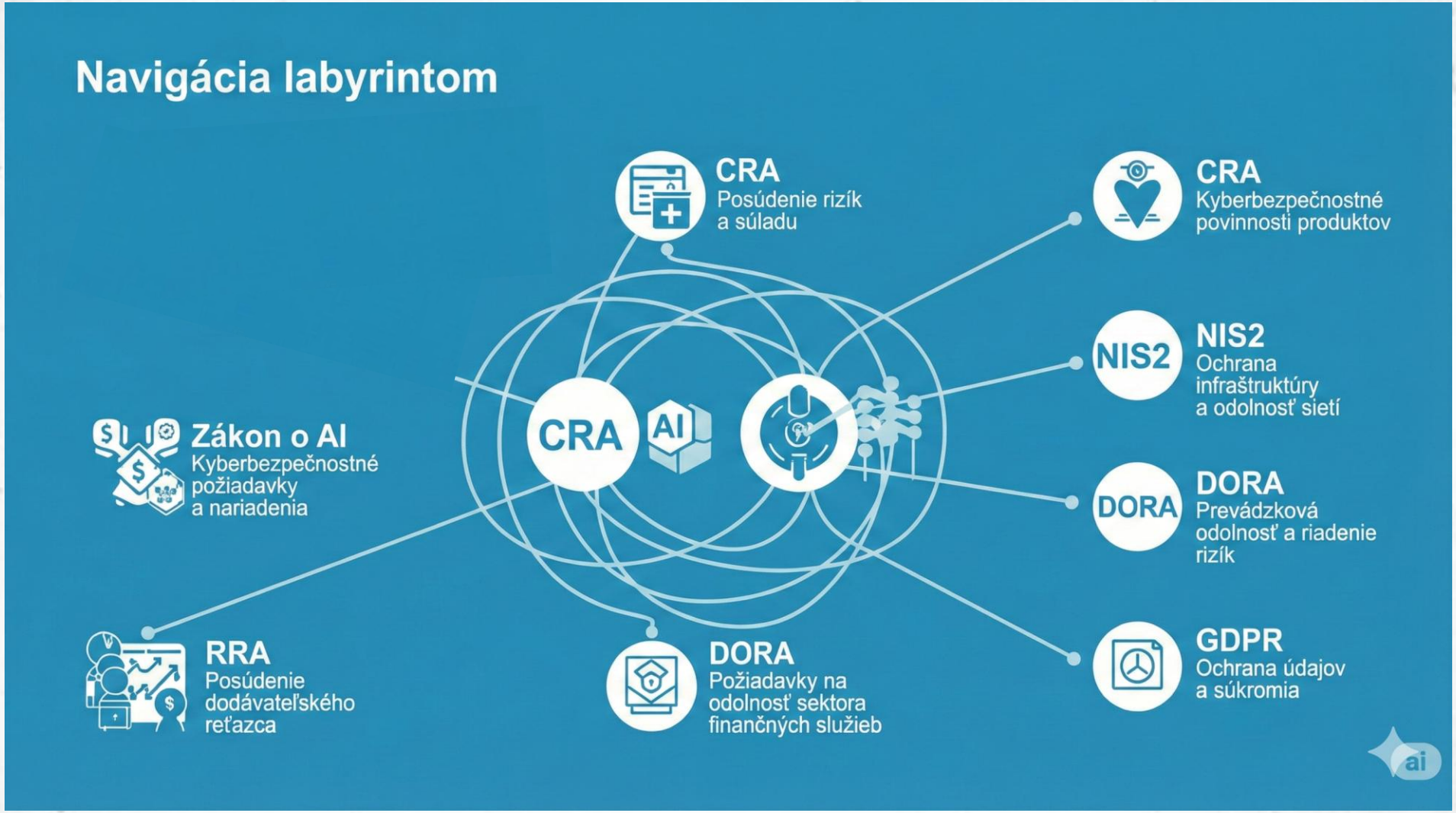
Smernica NIS2 (III.)

- smernica sa musí transponovať do právneho poriadku (nariadenie platí priamo)
- členské štáty mali transponovať smernicu do 17. októbra 2024 (SR – od 1.1.2025)
- implementácia do právnej úpravy v členských štátoch - organizácie sa musia prispôsobiť až po prijatí v danej krajine



Zdroj: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

Akt o kybernetickej bezpečnosti (I.)

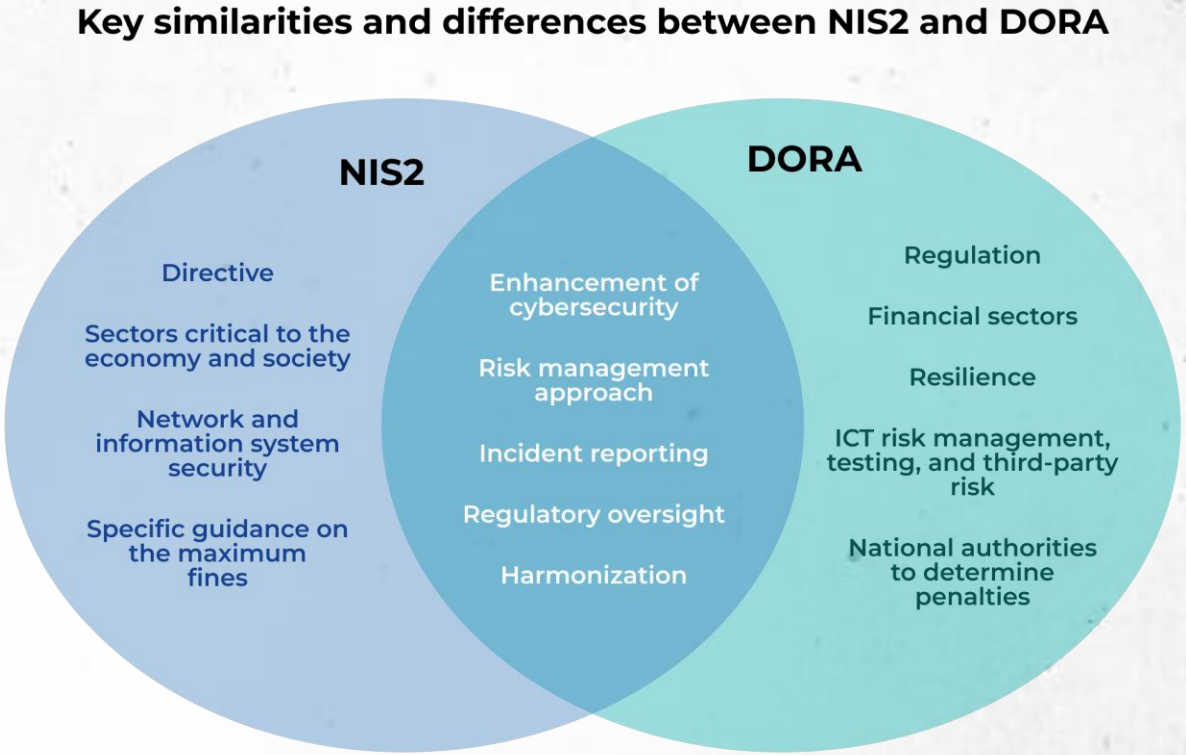


Zdroj: https://www.linkedin.com/pulse/navigating-labyrinth-in-depth-analysis-red-cra-ai-act-faenzi-edcdf/

Nariadenie DORA

- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554** o digitálnej prevádzkovej odolnosti finančného sektora (DORA)
- https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32022R2554

- digitálna prevádzková odolnosť finančného sektora
- riadenie ICT rizík, testovanie, hlásenie incidentov
- dohľad nad tretími stranami (ICT poskytovatelia)



Zdroj: https://advisera.com/articles/nis2-and-dora-similarities-and-differences/

Nariadenie GDPR

- NARIADENIE EURÓPSKEHO PARLAMENTU A RADY **(EÚ) 2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (**všeobecné nariadenie o ochrane údajov - GDPR**)

- **článok 32 – Bezpečnosť spracúvania**
- prevádzkovateľ a sprostredkovateľ sú povinní:
  - posúdiť **riziká pre práva a slobody dotknutých osôb**
  - prijať opatrenia primerané:
    - povahe spracúvania
    - rozsahu a účelu spracúvania
    - pravdepodobnosti a závažnosti rizika
  - bezpečnostné opatrenia:
    - pseudonymizácia a šifrovanie osobných údajov
    - schopnosť zabezpečiť: dôvernosť (confidentiality) integritu (integrity) dostupnosť (availability) odolnosť systémov a služieb
    - schopnosť obnovy dostupnosti údajov po incidente
    - pravidelné testovanie, hodnotenie a posudzovanie účinnosti opatrení

Akt o kybernetickej bezpečnosti

- **Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881** zo 17. apríla 2019 o agentúre ENISA (Agentúra 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 – EU CyberSecurity Act)**
- https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32019R0881

- posilnil mandát agentúry ENISA
- zaviedol rámec európskej certifikácie kybernetickej bezpečnosti
- zameranie na produkty, služby a procesy IKT
- základ pre dôveryhodnosť digitálneho trhu EÚ

Akt o kybernetickej solidarite

- **Nariadenie** Európskeho parlamentu a Rady (EÚ) **2025/38** z 19. decembra 2024, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 **(akt o kybernetickej solidarite)**
- https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32025R0038

- posilnenie schopností EÚ reagovať na veľké incidenty
- tri piliere:
  - Európsky systém kybernetických varovaní
  - mechanizmus kybernetickej núdzovej reakcie
  - mechanizmus hodnotenia incidentov
- podpora koordinovanej reakcie na krízy

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 – Cyber Resilience Act**)
- https://eur-lex.europa.eu/eli/reg/2024/2847/oj/slk

- zvýšiť kybernetickú bezpečnosť v celej EÚ stanovením povinných požiadaviek na **kybernetickú bezpečnosť produktov s digitálnymi prvkami.**
- podporovať bezpečné postupy tým, že sa budú výrobcovia nabádať, aby kybernetickú bezpečnosť začlenili do **fáz návrhu a vývoja produktov**.

- platí pre hardvér aj softvér
- bezpečnosť „by design“ a „by default“
- povinné riadenie zraniteľností počas životného cyklu produktu
- povinnosť hlásiť:
  - aktívne zneužívané zraniteľnosti
  - závažné kybernetické incidenty

Vývoj právnej úpravy v SR (I.)

- **Historický vývoj**
  - zákon č. 215/2002 Z. z. o elektronickom podpise
  - zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov,
  - zákon č. 610/2003 Z. z. o elektronických komunikáciách v znení neskorších predpisov,
  - zákon č. 22/2004 Z. z. o elektronickom obchode
  - zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností
  - zákon č. 300/2005 Z. z. trestný zákon v znení neskorších predpisov,
  - zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy

  - uznesenie vlády SR č. 570/2008 - Národná stratégia pre informačnú bezpečnosť v SR
  - uznesenie vlády SR č. 479/2009 – vznik jednotky CSIRT - CSIRT.SK

  - **Legislatívny zámer zákona o informačnej bezpečnosti** (rok 2010)

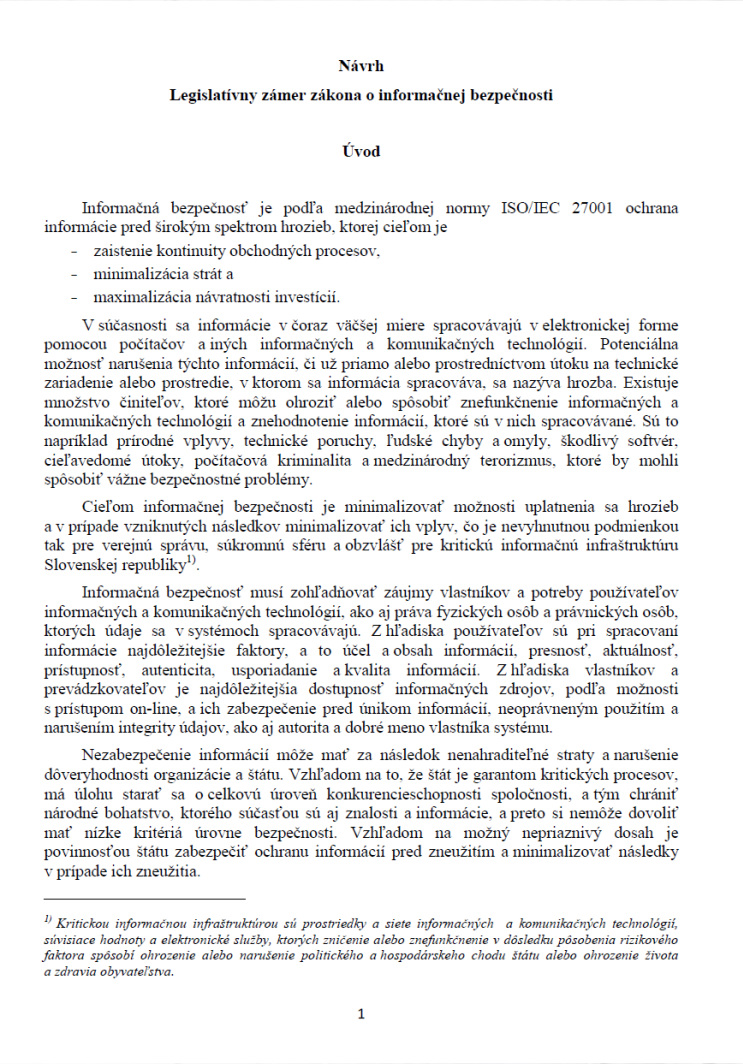
  - zákon č. 69/2018 Z. z. o **kybernetickej bezpečnosti**

Vývoj právnej úpravy v SR (II.)

- **Legislatívny zámer zákona o informačnej bezpečnosti**
  - rok 2010
  - cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru SR

  - Ministerstvo financií je v súčasnosti poverené uznesením vlády č. 570/2008 zosúladiť v spolupráci s Ministerstvom kultúry Slovenskej republiky legislatívnu terminológiu pre oblasť informatizácie spoločnosti, do ktorej spadá aj terminológia informačnej bezpečnosti.

  - kategorizácia informačných systémov verejnej správy
  - jednotka pre riešenie počítačových incidentov (CSIRT.SK) v SR
  - štandardizácia



Návrh

Legislatívny zámer zákona o informačnej bezpečnosti

Úvod

Informačná bezpečnosť je podľa medzinárodnej normy ISO/IEC 27001 ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je

- zaistenie kontinuity obchodných procesov,
- minimalizácia strát a
- maximalizácia návratnosti investícií.

V súčasnosti sa informácie v čoraz väčšej miere spracovávajú v elektronickej forme pomocou počítačov a iných informačných a komunikačných technológií. Potenciálna možnosť narušenia týchto informácií, či už priamo alebo prostredníctvom útoku na technické zariadenie alebo prostredie, v ktorom sa informácia spracováva, sa nazýva hrozba. Existuje množstvo činiteľov, ktoré môžu ohroziť alebo spôsobiť znefunkčnenie informačných a komunikačných technológií a znehodnotenie informácií, ktoré sú v nich spracovávané. Sú to napríklad prírodné vplyvy, technické poruchy, ľudské chyby a omyly, škodlivý softvér, cieľavedomé útoky, počítačová kriminalita a medzinárodný terorizmus, ktoré by mohli spôsobiť vážne bezpečnostné problémy.

Cieľom informačnej bezpečnosti je minimalizovať možnosti uplatnenia sa hrozieb a v prípade vzniknutých následkov minimalizovať ich vplyv, čo je nevyhnutnou podmienkou tak pre verejnú správu, súkromnú sféru a obzvlášť pre kritickú informačnú infraštruktúru Slovenskej republiky[1)].

Informačná bezpečnosť musí zohľadňovať záujmy vlastníkov a potreby používateľov informačných a komunikačných technológií, ako aj práva fyzických osôb a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska používateľov sú pri spracovaní informácie najdôležitejšie faktory, a to účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejšia dostupnosť informačných zdrojov, podľa možnosti s prístupom on-line, a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

Nezabezpečenie informácií môže mať za následok nenahraditeľné straty a narušenie dôveryhodnosti organizácie a štátu. Vzhľadom na to, že štát je garantom kritických procesov, má úlohu starať sa o celkovú úroveň konkurencieschopnosti spoločnosti, a tým chrániť národné bohatstvo, ktorého súčasťou sú aj znalosti a informácie, a preto si nemôže dovoliť mať nízke kritériá úrovne bezpečnosti. Vzhľadom na možný nepriaznivý dosah je povinnosťou štátu zabezpečiť ochranu informácií pred zneužitím a minimalizovať následky v prípade ich zneužitia.

[1)] Kritickou informačnou infraštruktúrou sú prostriedky a siete informačných a komunikačných technológií, súvisiace hodnoty a elektronické služby, ktorých zničenie alebo znefunkčnenie v dôsledku pôsobenia rizikového faktora spôsobí ohrozenie alebo narušenie politického a hospodárskeho chodu štátu alebo ohrozenie života a zdravia obyvateľstva.

1

Zákon o kybernetickej bezpečnosti (I.)

- Zákon č. 69/2018 Z. z. o **kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov
- Predmet zákona (§1):
- podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä
  - postavenie a povinnosti prevádzkovateľa základnej služby,
  - bezpečnostné opatrenia,
  - hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
  - riešenie kybernetického bezpečnostného incidentu,
  - opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,
- správu v oblasti kybernetickej bezpečnosti
- organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“)
- audit kybernetickej bezpečnosti a dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona

28.11.2024 12:05 | Bezpečnosť

Úroveň kybernetickej bezpeč sa zvýši

Zdroj: istock

TASR

Novela bude účinná od 1. januára 2

Zvýšenie úrovne kybernetickej bezpečnosti

rizík, ktoré sú spôsobené rýchlym technologickým vývojom a

Ako ovplyvní smernica NIS2 možnosť používať druhotný softvér?

redakcia touchIT 25. februára 2025

Tento článok je tlačová správa a je publikovaný bez redakčných úprav.

V decembri 2022 schválila Európska únia smernicu NIS2 (Network and Information System Directive 2), ktorá stanovuje pravidlá a požiadavky na kybernetickú bezpečnosť ICT systémov a sietí. Členské štáty EÚ mali implementovať NIS2 do svojich právnych poriadkov do 18. októbra 2024. Na Slovensku smernica nadobudla účinnosť 1. januára 2025. Ovplyvnia nové prísnejšie pravidlá

znosť používania druhotného softvéru?

nyc digitalizáciou. To sú hlavné ciele novely zákona o kybernetickej

platná od 16. januára 2023.

Zdroj: https://zive.aktuality.sk/clanok/zpNPdfB/uroven-kybernetickej-bezpecnosti-na-slovensku-sa-zvysi/, https://touchit.sk/ako-ovplyvni-smernica-nis2-moznost-pouzivat-druhotny-softver/698207, https://touchit.sk/je-vasa-firma-pripravena-na-nis2/620047, https://zive.aktuality.sk/clanok/JExEku3/prezident-podpisal-novelu-zakona-o-kybernetickej-bezpecnosti-co-sa-meni/

Zákon o kybernetickej bezpečnosti (III.)

- novela zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

- rozšírenie povinných subjektov
- zrušenie dopadových a špecifických kritérií
- bezpečnosť dodávateľského reťazca

- neboli novelizované vykonávacie právne predpisy, resp. osobitná právna úprava

13.12.2024 18:40 | Bezpečnosť

Prezident podpísal novelu zákona o kybernetickej bezpečnosti, čo sa mení

Zdroj: istock

živě

TASR

Novela bude účinná od 1. januára 2025.

Zdroj: https://zive.aktuality.sk/clanok/JExEku3/prezident-podpisal-novelu-zakona-o-kybernetickej-bezpecnosti-co-sa-meni/

Zákon o kybernetickej bezpečnosti (IV.)

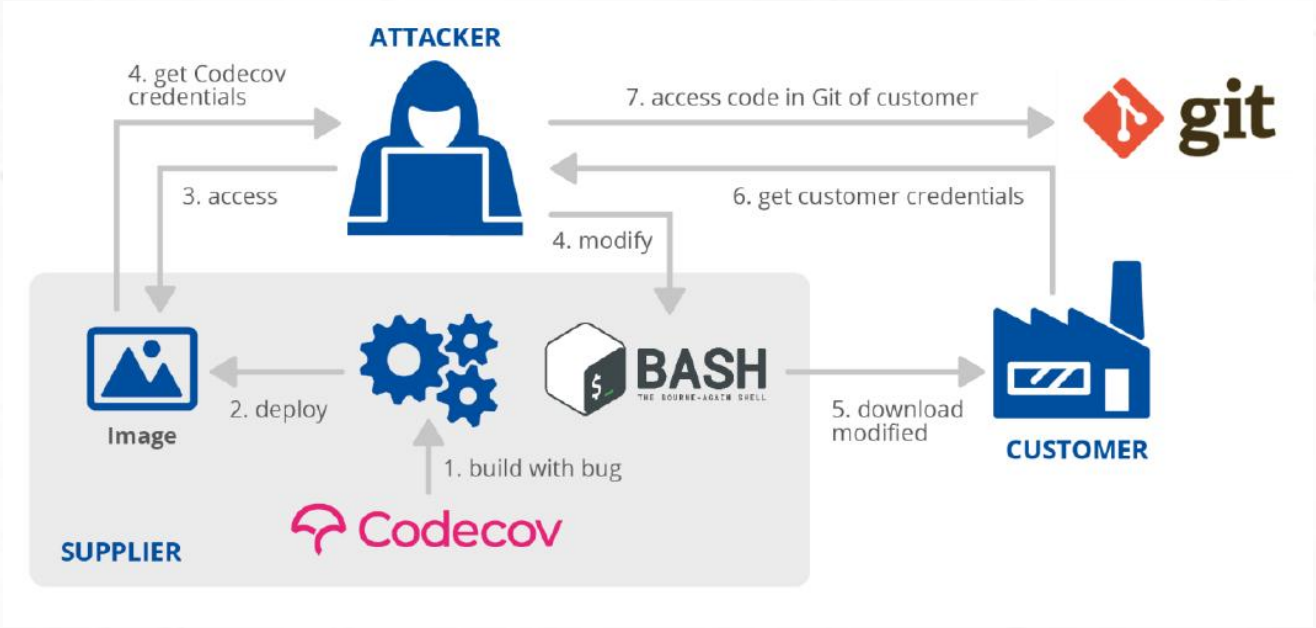
- § 17 ods. 1 písm. e) zákona o KB - osoba, ktorá spĺňa najmenej podmienky **veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 zákona o KB

- odporúčanie Komisie 2003/361/ES
- **viac ako 50** zamestnancov a
- obrat alebo súvaha **nad 10 mil. €**

Zdroj: https://www.nbu.gov.sk/novela-kyberzakona-je-predo-dvermi-nbu-zverejnil-pomocku-pre-organizacie/

Zákon o kybernetickej bezpečnosti (V.)

- rozšírenie pôsobnosti na **dodávateľské reťazce**
- § 17 ods. 1 písm. i) zákona o KB - tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu



Zdroj: https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html

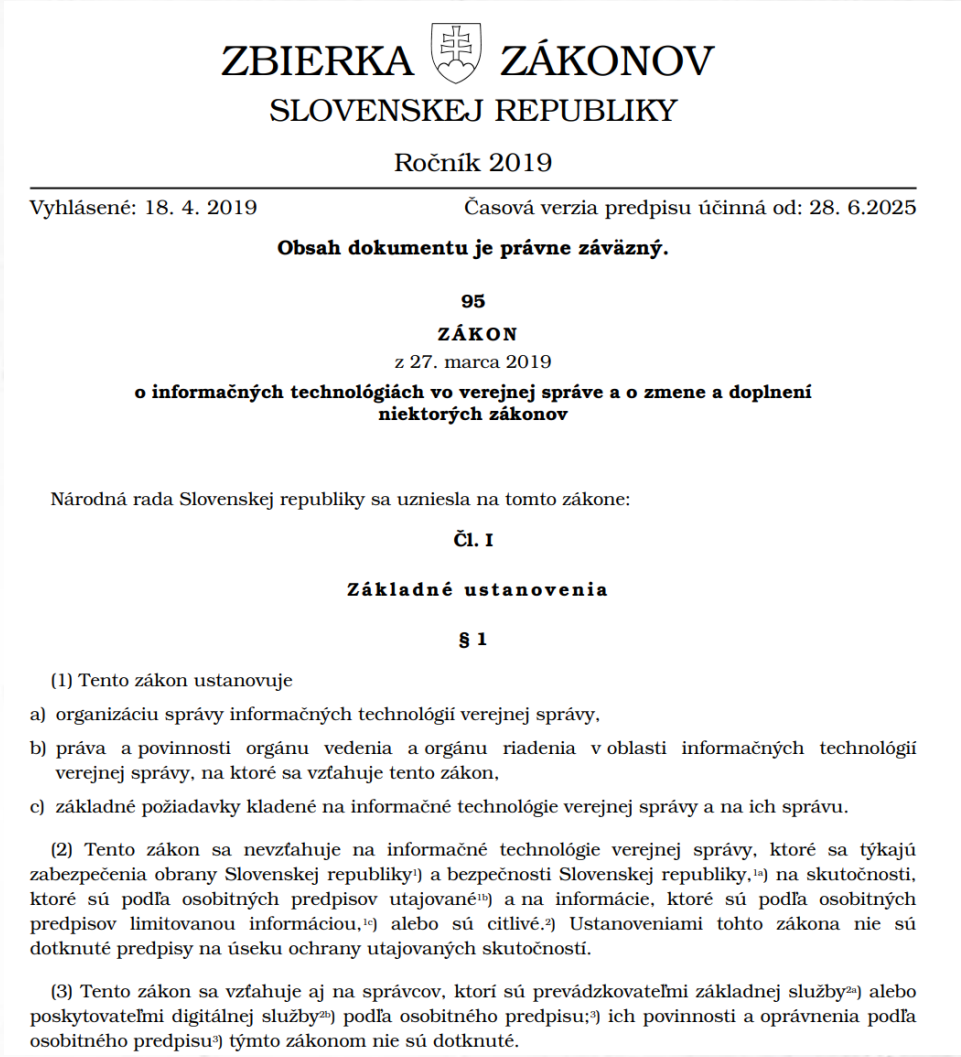
Vykonávacie predpisy k zákonu o KB

Vykonávacie právne predpisy:

- Vyhláška NBÚ č. **166/2018 Z. z.**, o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- Vyhláška NBÚ č. **492/2022 Z. z.**, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
- Vyhláška NBÚ č. **493/2022 Z. z.**, o audite kybernetickej bezpečnosti
- Vyhláška NBÚ č. **264/2023 Z. z.**, ktorou sa mení a dopĺňa vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Vyhláška NBÚ č. **226/2025 Z. z.**, ktorou sa ustanovujú podrobnosti o hláseniach
- Vyhláška NBÚ č. **227/2025 Z. z.**, o bezpečnostných opatreniach

Zákon o ITVS (I.)

- **zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a** o zmene a doplnení niektorých zákonov (**zákon o ITVS**)
- je sektorová právna úprava (lex specialis)
- cieľom zákona o ITVS je komplexné a jednotné riadenie IT - od plánovania a organizácie cez implementáciu a prevádzku až po monitoring a hodnotenie
- zákon sa nezameriava výlučne na kybernetickú bezpečnosť, ale na celý životný cyklus riadenia ITVS
- ustanovuje jednotné vedenie a riadenie IT vo verejnej správe



ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2019

Vyhlásené: 18. 4. 2019 Časová verzia predpisu účinná od: 28. 6.2025

Obsah dokumentu je právne záväzný.

95

ZÁKON

z 27. marca 2019

o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

Základné ustanovenia

§ 1

(1) Tento zákon ustanovuje

a) organizáciu správy informačných technológií verejnej správy,

b) práva a povinnosti orgánu vedenia a orgánu riadenia v oblasti informačných technológií verejnej správy, na ktoré sa vzťahuje tento zákon,

c) základné požiadavky kladené na informačné technológie verejnej správy a na ich správu.

(2) Tento zákon sa nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky[1]) a bezpečnosti Slovenskej republiky,[1a]) na skutočnosti, ktoré sú podľa osobitných predpisov utajované[1b]) a na informácie, ktoré sú podľa osobitných predpisov limitovanou informáciou,[1c]) alebo sú citlivé.[2]) Ustanoveniami tohto zákona nie sú dotknuté predpisy na úseku ochrany utajovaných skutočností.

(3) Tento zákon sa vzťahuje aj na správcov, ktorí sú prevádzkovateľmi základnej služby[2a]) alebo poskytovateľmi digitálnej služby[2b]) podľa osobitného predpisu;[3]) ich povinnosti a oprávnenia podľa osobitného predpisu[3]) týmto zákonom nie sú dotknuté.

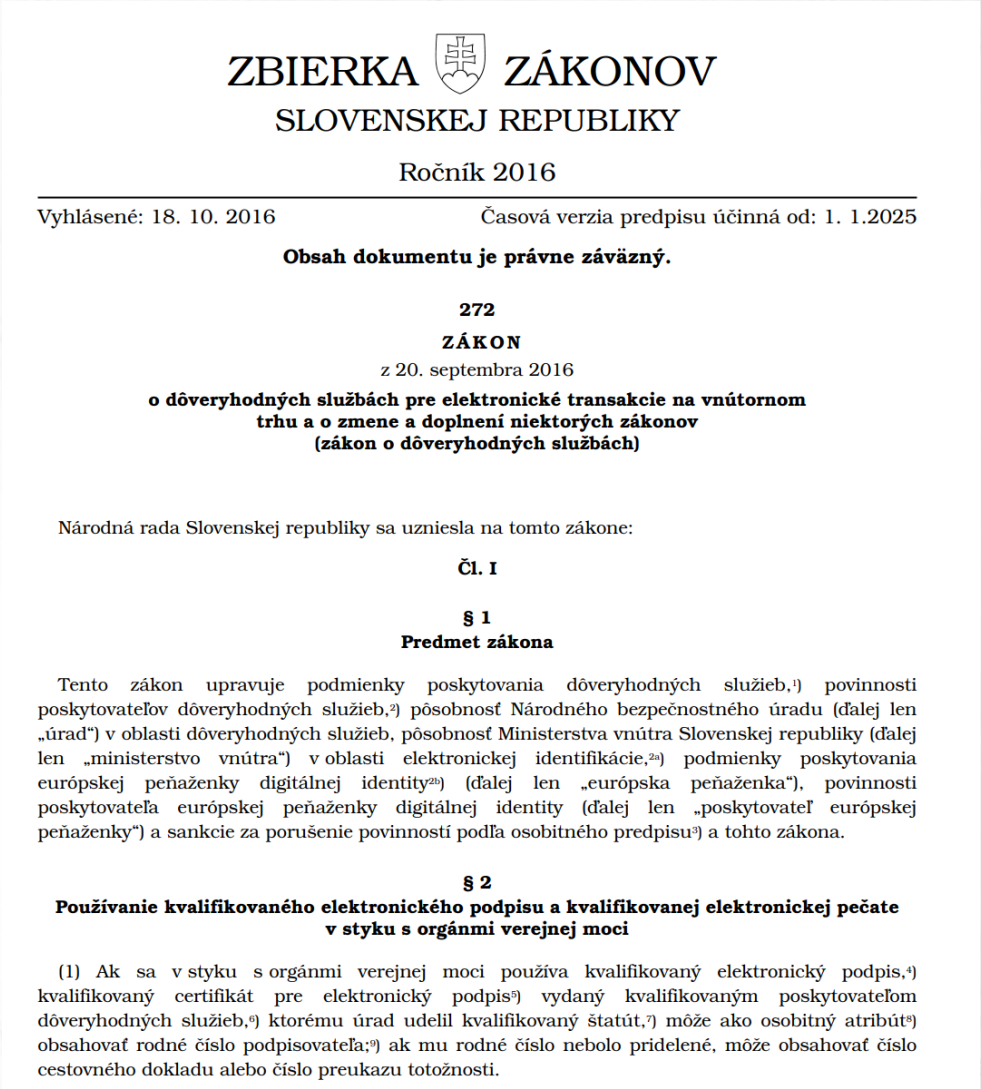
Zákon o ITVS (II.)

Vykonávacie právne predpisy:

- Vyhláška ÚPVII **č. 78/2020 Z. z.** o štandardoch pre informačné technológie verejnej správy,
- Vyhláška ÚPVII **č. 179/2020 Z. z.**, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- Vyhláška MIRRI **č. 333/2022 Z. z.** o elektronizácii agendy verejnej správy,
- Vyhláška MIRRI **č. 401/2023 Z. z.** o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

Ďalšia právna úprava (I.)

- **Zákon č. 272/2016 Z. z.** o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov **(zákon o dôveryhodných službách)**
  - národná úprava dopĺňajúca **nariadenie eIDAS**
  - upravuje:
    - podmienky poskytovania dôveryhodných služieb
    - povinnosti poskytovateľov dôveryhodných služieb
  - relevancia pre kybernetickú bezpečnosť:
    - bezpečnosť certifikátov, elektronických podpisov a pečatí
    - dôveryhodnosť a integrita elektronických transakcií



ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2016

Vyhlásené: 18. 10. 2016 Časová verzia predpisu účinná od: 1. 1.2025

Obsah dokumentu je právne záväzný.

272

ZÁKON

z 20. septembra 2016

o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

§ 1
Predmet zákona

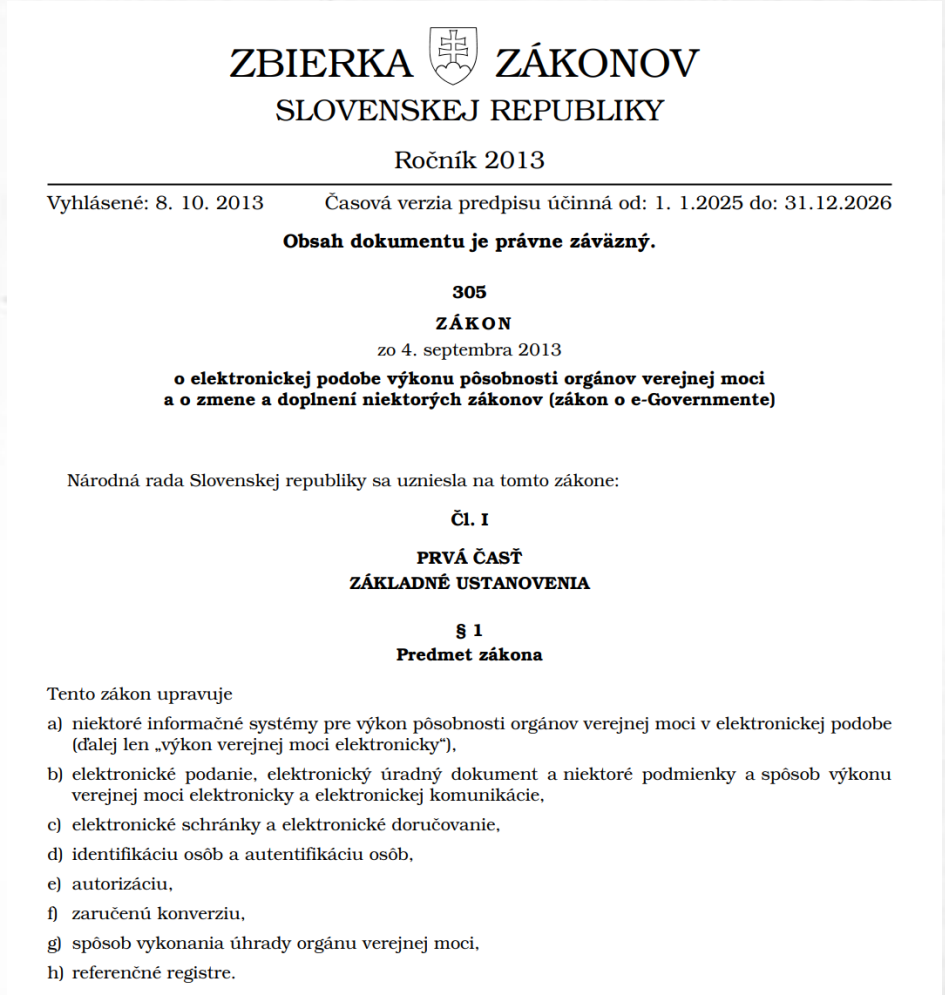
Tento zákon upravuje podmienky poskytovania dôveryhodných služieb,[1] povinnosti poskytovateľov dôveryhodných služieb,[2] pôsobnosť Národného bezpečnostného úradu (ďalej len „úrad") v oblasti dôveryhodných služieb, pôsobnosť Ministerstva vnútra Slovenskej republiky (ďalej len „ministerstvo vnútra") v oblasti elektronickej identifikácie,[2a] podmienky poskytovania európskej peňaženky digitálnej identity[2b] (ďalej len „európska peňaženka"), povinnosti poskytovateľa európskej peňaženky digitálnej identity (ďalej len „poskytovateľ európskej peňaženky") a sankcie za porušenie povinností podľa osobitného predpisu[3] a tohto zákona.

§ 2
Používanie kvalifikovaného elektronického podpisu a kvalifikovanej elektronickej pečate v styku s orgánmi verejnej moci

(1) Ak sa v styku s orgánmi verejnej moci používa kvalifikovaný elektronický podpis,[4] kvalifikovaný certifikát pre elektronický podpis[5] vydaný kvalifikovaným poskytovateľom dôveryhodných služieb,[6] ktorému úrad udelil kvalifikovaný štatút,[7] môže ako osobitný atribút[8] obsahovať rodné číslo podpisovateľa;[9] ak mu rodné číslo nebolo pridelené, môže obsahovať číslo cestovného dokladu alebo číslo preukazu totožnosti.

Ďalšia právna úprava (II.)

- **Zákon č. 305/2013 Z. z.** o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov **(zákon o e-Governmente)**
  - upravuje výkon verejnej moci **elektronickou formou**
  - kľúčové oblasti:
    - elektronické podania a úradné dokumenty
    - elektronické schránky a doručovanie
    - identifikácia, autentifikácia a autorizácia
    - zaručená konverzia
  - parciálna úprava kybernetickej bezpečnosti v prostredí verejnej správy



ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2013

Vyhlásené: 8. 10. 2013 Časová verzia predpisu účinná od: 1. 1.2025 do: 31.12.2026

Obsah dokumentu je právne záväzný.

305

ZÁKON

zo 4. septembra 2013

o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

PRVÁ ČASŤ
ZÁKLADNÉ USTANOVENIA

§ 1
Predmet zákona

Tento zákon upravuje

a) niektoré informačné systémy pre výkon pôsobnosti orgánov verejnej moci v elektronickej podobe (ďalej len „výkon verejnej moci elektronicky“),

b) elektronické podanie, elektronický úradný dokument a niektoré podmienky a spôsob výkonu verejnej moci elektronicky a elektronickej komunikácie,

c) elektronické schránky a elektronické doručovanie,

d) identifikáciu osôb a autentifikáciu osôb,

e) autorizáciu,

f) zaručenú konverziu,

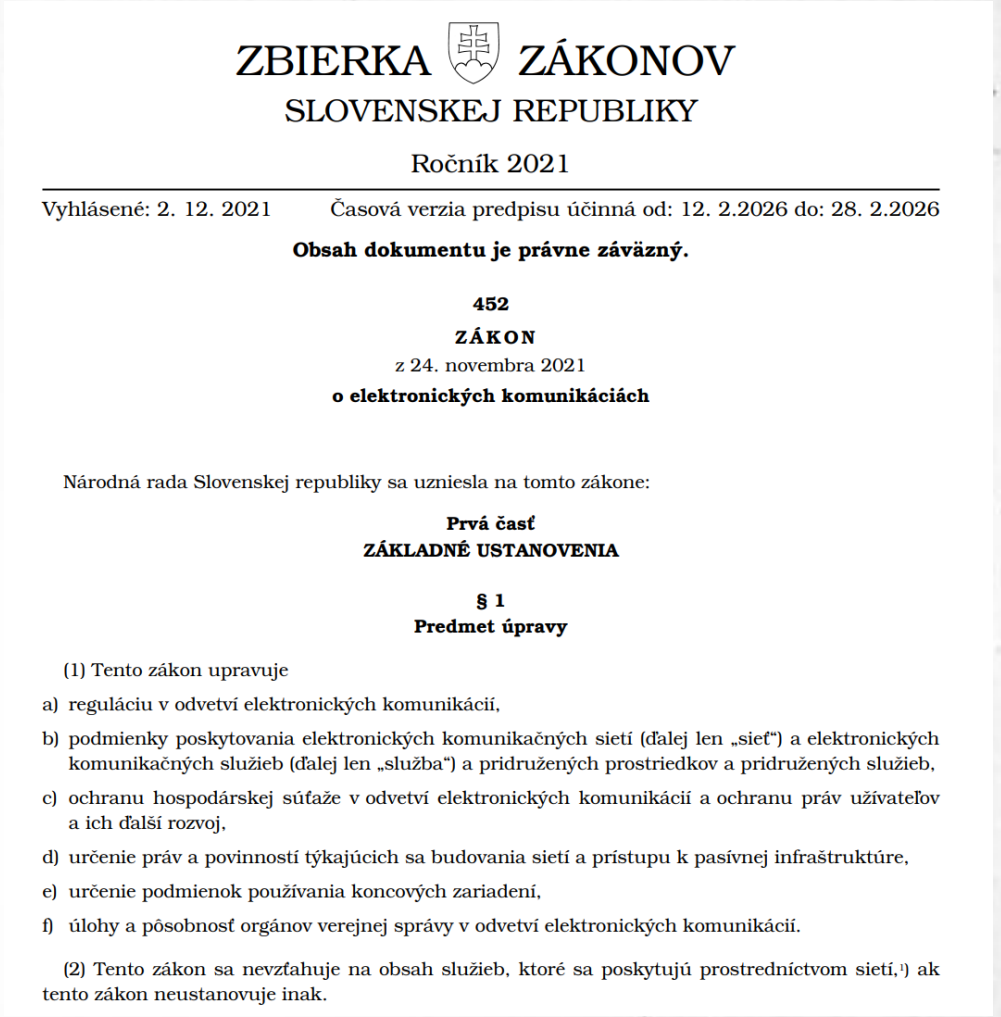
g) spôsob vykonania úhrady orgánu verejnej moci,

h) referenčné registre.

Ďalšia právna úprava (III.)

- **Zákon č. 452/2021 Z. z. o elektronických komunikáciách**
  - regulácia elektronických komunikačných sietí a služieb
  - bezpečnosť a integrita sietí (štvrtá časť zákona)
  - povinnosti podnikov:
    - technické a organizačné opatrenia
    - riešenie bezpečnostných incidentov
    - riadenie kontinuity činností
    - monitoring, audit, testovanie a šifrovanie
  - osobitná úprava ochrany súkromia a osobných údajov

- zákon **č. 18/2018** Z. z. o **ochrane osobných údajov** a o zmene a doplnení niektorých zákonov
- zákon **č. 367/2024** Z. z. **o kritickej infraštruktúre** a o zmene a doplnení niektorých zákonov
- zákon č. 215/2004 Z. z. o **ochrane utajovaných skutočností** a **o zmene a doplnení niektorých zákonov**



ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2021

Vyhlásené: 2. 12. 2021 Časová verzia predpisu účinná od: 12. 2.2026 do: 28. 2.2026

Obsah dokumentu je právne záväzný.

452

ZÁKON

z 24. novembra 2021

o elektronických komunikáciách

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Prvá časť
ZÁKLADNÉ USTANOVENIA

§ 1
Predmet úpravy

(1) Tento zákon upravuje

a) reguláciu v odvetví elektronických komunikácií,

b) podmienky poskytovania elektronických komunikačných sietí (ďalej len „sieť“) a elektronických komunikačných služieb (ďalej len „služba“) a pridružených prostriedkov a pridružených služieb,

c) ochranu hospodárskej súťaže v odvetví elektronických komunikácií a ochranu práv užívateľov a ich ďalší rozvoj,

d) určenie práv a povinností týkajúcich sa budovania sietí a prístupu k pasívnej infraštruktúre,

e) určenie podmienok používania koncových zariadení,

f) úlohy a pôsobnosť orgánov verejnej správy v odvetví elektronických komunikácií.

(2) Tento zákon sa nevzťahuje na obsah služieb, ktoré sa poskytujú prostredníctvom sietí,[1]) ak tento zákon neustanovuje inak.

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

meno.priezvisko@upjs.sk

https://cyberawareness.sk