

PRÁVNÁ ANALÝZA SÚČASNÉHO STAVU PRÁVNEJ ÚPRAVY KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE

Zadávatel':

Odbor: Odbor riadenia kybernetickej a informačnej bezpečnosti
Sekcia kybernetickej bezpečnosti
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Vypracovali: JUDr. Jozef Andraško, PhD.
JUDr. Matúš Mesarčík, PhD., LL.M

Verzia:	Posledná zmena
1.0	30.6.2022

ZOZNAM SKRATIEK

AIA znamená Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (Akt o umelej inteligencii) a menia niektoré legislatívne akty únie.

Akt o kybernetickej bezpečnosti znamená 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.

DSA znamená návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o jednotnom trhu s digitálnymi službami (akt o digitálnych službách) a o zmene smernice 2000/31/ES.

DMA znamená návrh nariadenia Európskeho parlamentu a Rady o súťažeschopných a spravodlivých trhoch digitálneho sektora (akt o digitálnych trhoch).

Nariadenie eIDAS znamená nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

EÚ znamená Európska únia.

GDPR znamená 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) (Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88).

MIRRI znamená Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.

Nariadenie DORA znamená návrh nariadenie Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014 (COM/2020/595 final).

Návrh smernice o odolnosti kritických subjektov znamená návrh smernice Európskeho parlamentu a Rady o odolnosti kritických subjektov. COM(2020) 829 final 2020/0365(COD).

Návrh smernice NIS 2 znamená návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 (COM/2020/823 final).

NBÚ znamená Národný bezpečnostný úrad Slovenskej republiky

PZS znamená prevádzkovateľ základných služieb

Smernica NIS znamená 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 (Ú. v. EÚ L 194, 19.7.2016, s. 1 – 30).

Smernica o európskej kritickej infraštruktúre znamená smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu.

SR znamená Slovenská republika.

Vyhláška č. 164/2018 Z. z. znamená vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby)

Vyhláška č. 165/2018 Z. z. znamená vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

Vyhláška č. 362/2018 Z. z. znamená vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Vyhláška č. 436/2019 Z. z. znamená vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

Vyhláška č. 179/2020 Z. z. znamená vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

ZoITVS znamená zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

ZoKB znamená zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

OBSAH

1. ÚVOD	7
2. KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE JEDNOTNÉHO DIGITÁLNEHO TRHU EURÓPSKEJ ÚNIE	8
2.1 Stratégia EÚ v oblasti kybernetickej bezpečnosti.....	8
2.2 Jednotný digitálny trh a súvisiaca právna úprava	8
2.2.1. Ochrana osobných údajov	11
2.2.1.1. Pôsobnosť GDPR	11
2.2.1.2. Kybernetická bezpečnosť	14
2.2.2. Umelá inteligencia	19
2.2.2.1. Pôsobnosť	19
2.2.2.2. Kybernetická bezpečnosť	22
2.2.3. Sociálne média	24
2.2.3.1. Pôsobnosť	24
2.2.3.2. Kybernetická bezpečnosť	25
2.2.4. Elektronická identifikácia	27
2.2.4.1. Pôsobnosť	27
2.2.4.2. Kybernetická bezpečnosť	28
2.2.5. Smernica NIS.....	29
2.2.5.1. Pôsobnosť	30
2.2.5.2. Kybernetická bezpečnosť	31
2.2.6. Akt o kybernetickej bezpečnosti	33
2.2.6.1. Pôsobnosť	33
2.2.6.2. Kybernetická bezpečnosť	34
2.2.7. Návrh smernice NIS 2	36
2.2.7.1. Pôsobnosť	36
2.2.7.2. Kybernetická bezpečnosť	39
2.2.7.3. Bezpečnostné opatrenia	40
2.2.8. Návrh smernice o odolnosti kritických subjektov.....	42
2.2.8.1. Pôsobnosť	43
2.2.8.2. Kybernetická bezpečnosť	45
3. PRÁVNA ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE	48
3.1. Predmet a pôsobnosť právnej úpravy	48
3.1.1. Zákon o kybernetickej bezpečnosti	48
3.1.1.1. Základné služby a prevádzkovateľ základných služieb	50
3.1.1.2. Identifikácia prevádzkovateľov základných služieb	51
3.1.2. Zákon o informačných technológiách vo verejnej správe.....	52
3.1.2.1. Vzťah ZoKB a ZoITVS	54

3.1.3.	Identifikované problémy a návrhy riešení	55
3.1.3.1.	Zaradzovanie správcov do registra PZS v rozpore so smernicou NIS	55
3.1.3.2.	Neúplný zoznam orgánov riadenia vo vyhláške č. 179/2020 Z. z.	57
3.1.3.3.	Zoznam základných služieb pre podsektor informačné systémy verejnej správy.....	58
3.2.	Základné pojmy	59
3.2.1.	Identifikované problémy a návrhy riešení	70
3.2.1.1.	Pojem kybernetická bezpečnosť v kontexte ZoITVS	70
3.2.1.2.	Terminologické nedostatky	73
3.3.	Bezpečnostné incidenty	74
3.3.1.	Zákon o kybernetickej bezpečnosti	74
3.3.2.	Zákon o informačných technológiách vo verejnej správe.....	75
3.3.3.	Identifikované problémy a návrhy riešení	76
3.3.3.1.	Kybernetické bezpečnostné incidenty, ktoré nie sú závažné	76
3.3.3.2.	Chýbajúca lehota.....	77
3.3.3.3.	Rozšírenie osobnej pôsobnosti správcov, ktorí nahlásujú kybernetické bezpečnostné incidenty podľa ZoITVS	78
3.4.	Bezpečnostné opatrenia.....	78
3.4.1.	Zákon o kybernetickej bezpečnosti	79
3.4.2.	Zákon o informačných technológiách vo verejnej správe.....	80
3.4.3.	Porovnanie bezpečnostných opatrení.....	80
3.4.4.	Identifikované problémy a návrhy riešení	128
3.5.	Dozor a dohľad.....	131
3.5.1.	Zákon o kybernetickej bezpečnosti	131
3.5.1.1.	NBÚ SR a dohľad	132
3.5.1.2.	Jednotky CSIRT a ich úlohy.....	137
3.5.2.	Zákon o informačných technológiách vo verejnej správe.....	140
3.5.3.	Identifikované problémy a návrhy riešení	145
3.6.	Sankcie	147
3.6.1.	Zákon o kybernetickej bezpečnosti	147
3.6.2.	Zákon o informačných technológiách vo verejnej správe.....	151
3.6.3.	Identifikované problémy a návrhy riešení	153
4.	KONCEPČNÉ NÁVRHY A ALTERNATÍVY RIEŠENÍ IDENTIFIKOVANÝCH PROBLÉMOV	154
4.1	Ponechať status quo	154
4.2	Koncipovanie komplexnej právnej úpravy v jednom zákone	154
4.3	Ponechať dva zákony a novelizovať ich s cieľom čo najväčšej previazanosti ..	155
PRÍLOHA.....		157

1. ÚVOD

Právna úprava kybernetickej bezpečnosti je predmetom dynamického vývoja. Nejde len o vplyvy externých faktorov ako pandémie COVID-19 či vojenský konflikt na Ukrajine, ale potrebu revízie regulácie danej oblasti zvyrazňuje aj líder digitálnych politík – Európska únia.

Z týchto dôvodov plne rozumieme zadaniu, ktorého základným cieľom je zmapovať legislatívu kybernetickej bezpečnosti v Slovenskej republike a navrhnúť čiastkové či koncepčné riešenia. Z metodologického hľadiska sme k danej úlohe pristúpili nasledovným spôsobom. Po tomto úvode nasleduje druhá časť analýzy, ktorá dáva reguláciu kybernetickej bezpečnosti do kontextu jednotného digitálneho trhu EÚ. Považujeme za nevyhnutné reflektovať legislatívu, ktorá sa digitálneho trhu EÚ týka, nakoľko obsahuje viacero povinností týkajúcich sa kybernetickej bezpečnosti. Zároveň nemožno právnú úpravu kybernetickej bezpečnosti vnímať izolovane, ale ako súčasť komplexného regulačného celku. Z týchto dôvodov sa bližšie venujeme strategickým dokumentom na úrovni EÚ, ochrane osobných údajov, regulácií umelej inteligencie, sociálnych sietí, elektronickej identifikácie či kritickej infraštruktúry. Pre lepšiu prehľadnosť ponúkame konkrétne prepojenia na oblasť kybernetickej bezpečnosti.

Tretia časť analýzy je ťažisková a venuje sa právnej úprave kybernetickej bezpečnosti na úrovni Slovenskej republiky. Vymedzili sme šesť oblastí, na ktoré sa zameriavame a porovnávame dané právne povinnosti v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**ZoKB**“) a zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „**ZoITVS**“). Sústredíme sa na pôsobnosť právnych predpisov, základné pojmy, kybernetické bezpečnostné incidenty, bezpečnostné opatrenia, dozor a dohľad a sankcie. Pri identifikovaní nedostatkov ponúkame rámcové odporúčanie na jeho odstránenie.

V poslednej, štvrtej časti sa zamýšľame nad rôznymi koncepčnými riešeniami právnej úpravy kybernetickej bezpečnosti v Slovenskej republike. Aj s ohľadom na identifikované nedostatky prezentujeme výhody a nevýhody komplexnej právnej úpravy v jednom zákone, ponechanie súčasného stavu a systému s dvoma zákonmi po odstránení nedostatkov.

2. KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE JEDNOTNÉHO DIGITÁLNEHO TRHU EURÓPSKEJ ÚNIE

2.1 Stratégia EÚ v oblasti kybernetickej bezpečnosti

Prvá stratégia EÚ v oblasti kybernetickej bezpečnosti bola prijatá v roku 2013 a stanovila strategické ciele a konkrétne opatrenia na dosiahnutie odolnosti, zníženie počítačovej kriminality, rozvoj politiky a kapacít kybernetickej obrany, rozvoj priemyselných a technologických zdrojov a vytvorenie koherentnej medzinárodnej politiky kybernetického priestoru pre Európsku úniu. **Stratégia kybernetickej bezpečnosti Európskej únie**¹ bola 7. februára 2013 predložená Vysokou predstaviteľkou Európskej únie pre zahraničné veci a bezpečnostnú politiku. Predmetná stratégia opisuje **kybernetickú bezpečnosť** nasledovne: „*Kybernetická bezpečnosť obyčajne odkazuje na ochranné opatrenia a plány, ktoré môžu byť použité k ochrane kybernetickej domény, a to ako v civilnej, tak aj vo vojenskej oblasti, pred hrozbami, ktoré sú s nimi spojené alebo ktoré by mohli poškodiť jej vzájomne prepojené siete a informačnú infraštruktúru. Kybernetická bezpečnosť usiluje o zachovanie dostupnosti a integrity sietí a infraštruktúry a dôveryhodnosť informácií v nich obsiahnutých.*“²

V roku 2020 bola predstavená **Stratégia kybernetickej bezpečnosti EÚ pre digitálnu dekádu**³, ktorej cieľom je posilniť kolektívnu odolnosť Európy proti kybernetickým hrozbám a pomôže zabezpečiť, aby mohli všetci občania a podniky plne využívať dôveryhodné a spoľahlivé služby a digitálne nástroje. Nová stratégia kybernetickej bezpečnosti sa zameriava na zabezpečenie globálneho a otvoreného internetu a zároveň zaistenie bezpečnosti, ako aj na ochranu európskych hodnôt a základných práv všetkých občanov. Predmetná stratégia obsahuje konkrétne návrhy regulačných, investičných a politických iniciatív v troch oblastiach činnosti EÚ:

- odolnosť, technologická suverenita a vedúce postavenie;
- budovanie operačnej kapacity na prevenciu, odrádzanie a reakciu;
- pokrok v globálnom a otvorenom kybernetickom priestore prostredníctvom intenzívnejšej spolupráce.⁴

2.2 Jednotný digitálny trh a súvisiaca právna úprava

Po vytvorení jednotného trhu Európskej únie je ďalším ambicióznym krokom vytvorenie jednotného digitálneho trhu. Ide taktiež o jednu z priorít súčasného vedenia Európskej komisie prezentovaných v plánoch a politických usmerneniach.⁵ Nakoľko ide o komplexnú problematiku, čiastkové ciele sú prezentované prostredníctvom oznámení, komuniké či strategických plánov.

¹ KOMISIA: Stratégia kybernetickej bezpečnosti Európskej únie. Brusel: 2013, s. 3.

² Tamtiež.

³ KOMISIA: Stratégia kybernetickej bezpečnosti EÚ pre digitálnu dekádu. Brusel: 2020.

⁴ Dostupné na: https://ec.europa.eu/commission/presscorner/detail/sk/ip_20_2391.

⁵ A Union that strives for more. My agenda for Europe. By candidate for President of the European Commission Ursula von der Leyen. Pozri hlavne bod 3 „A Europe fit for the digital age“. Dostupné na: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf.

Medzi najvýznamnejšie piliere v rámci akčných krokov pre kreovanie jednotného digitálneho trhu Európska Komisia zaraduje:

- Reguláciu čipov;⁶
- Reguláciu umelej inteligencie;⁷
- Európsku dátovú stratégiu a tvorbu dátových centier⁸
- Európsku priemyselnú stratégiu;⁹
- Vývoj vysoko výkonných počítačov;¹⁰
- Reguláciu digitálneho trhu;¹¹
- Európsku digitálnu identitu;¹²
- Podporu obranyschopnosti EÚ;¹³
- Otázky vesmíru;¹⁴
- Reguláciu digitálnych služieb;¹⁵
- **Kybernetickú bezpečnosť**;¹⁶
- Zlepšenie digitálnej gramotnosti¹⁷ a konektivity.¹⁸

Z hľadiska kybernetickej bezpečnosti špecifiká uvádza Stratégia kybernetickej bezpečnosti EÚ, ktorú analyzujeme vyššie. Dôvody zahrnutia oblasti kybernetickej bezpečnosti v rámci predmetného celku sú čiastočne načrtnuté v tzv. Digitálnom kompase do roku 2030,¹⁹ ktorý slúži na strategické plánovanie úloh aj v oblasti legislatívy. EÚ si uvedomuje, že práce na digitalizácii a súvisiacich otázkach musia byť nevyhnutne pružnejšie a rýchlejšie ako doteraz. Ako jeden z dôvodov kompasu uvádza aj pandémiu COVID-19: *„Pandémia...odhalila aj zraniteľné miesta nášho digitálneho priestoru, jeho zvýšenú závislosť od kritických technológií, ktoré často nepochádzajú z EÚ, poukázala na odkázanosť na malý počet veľkých technologických spoločností, zaznamenala nárast prílevu falšovaných výrobkov a kybernetických krádeží a zvýšila vplyv dezinformácií na naše demokratické spoločnosti.*²⁰

Otázky kybernetickej bezpečnosti sú vnímané hlavne z hľadiska dvoch strategických bodov kompasu. Po prvé, EÚ reflektuje na potrebu výchovy digitálne zručných obyvateľov

⁶ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

⁷ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en.

⁸ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

⁹ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.

¹⁰ Dostupné na: <https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing>.

¹¹ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

¹² Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

¹³ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en.

¹⁴ Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/space-eu-initiatives-satellite-based-connectivity-system-and-eu-approach-management-space-traffic_en.

¹⁵ Dostupné na: https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

¹⁶ Dostupné na: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>.

¹⁷ Dostupné na: <https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs>.

¹⁸ Dostupné na: <https://digital-strategy.ec.europa.eu/en/policies/connectivity>.

¹⁹ OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNŮV Digitálny kompas do roku 2030: digitálne desaťročie na európsky spôsob COM/2021/118 final. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52021DC0118>.

²⁰ Tamže, bod 2.

a vysokokvalifikovaných digitálnych odborníkov. S týmto cieľom je potrebná osвета ako prevencia pred úspešnými kybernetickými útokmi či inými škodlivými aktivitami na internete. Nedostatočné odborné kapacity sú ďalším z dôvodov implementácie daného cieľa do digitálneho kompasu: „*Digitálna odborná príprava a vzdelávanie by mali podporiť takých pracovníkov, ktorí si vedia osvojiť špecializované digitálne zručnosti na získanie kvalitného pracovného miesta a vybudovanie úspešnej kariéry. V roku 2019 pôsobilo v oblasti IKT 7,8 milióna odborníkov, s predchádzajúcou ročnou mierou rastu 4,2 %. Ak bude tento trend pokračovať, EÚ bude výrazne pod úrovňou predpokladanej potreby 20 miliónov odborníkov, napr. v kľúčových oblastiach, ako je **kybernetická bezpečnosť** alebo analýza údajov.*”²¹

Druhou oblasťou kľúčovou pre kybernetickú bezpečnosť je kreovanie bezpečných, výkonných a udržateľných digitálnych infraštruktúr.²²

Tieto otázky ale nie je možné vnímať samostatne, ale ako súčasť väčšieho celku, ktorým je jednotný digitálny trh. Z tohto dôvodu považujeme za vhodné túto časť analýzy venovať aj iným právnym rámcom, ktoré reguláciu kybernetickej bezpečnosti formujú resp. ovplyvňujú alebo budú významne ovplyvňovať v budúcnosti. Bližšie sa preto zameriavame na oblasť ochrany osobných údajov, umelej inteligencie, regulácie sociálnych médií, elektronickej identifikácie a kritickej infraštruktúry.

Úloha pre MIRRI

Monitorovať legislatívne procesy týkajúce sa nových strategických dokumentov a regulácie digitálneho trhu EÚ z dôvodu identifikovania potenciálnych konfliktných oblastí v legislatíve.

Zároveň považujeme za nevyhnutné upozorniť na to, že právo na kybernetickú bezpečnosť v súčasnosti nie je upravené ako základné ľudské právo a sloboda,²³ Európska Komisia predložila návrh Deklarácie digitálnych práv a princípov.²⁴ Predmetná deklarácia síce nebude súčasťou primárneho práva EÚ, ale pôjde o silné politické vyhlásenie, ktoré bude obsahovať niekoľko základných princípov, z ktorých musia konkrétne regulačné nástroje či už z dielne EÚ alebo národných členských štátoch vychádzať. Kapitulu V danej deklarácie tvoria záväzky v oblasti bezpečnosti, zabezpečenia a posilnenia postavenia. Deklarácia uvádza, že: „*každý by mal mať prístup k digitálnym technológiám, produktom a službám, ktoré sú bezpečné, zabezpečené a chránia súkromie už v štádiu návrhu.*”²⁵ Toto vyhlásenie je pretavené do dvoch konkrétnych záväzkov:

1. chrániť záujmy ľudí, podnikov a verejných inštitúcií pred počítačovou kriminalitou vrátane porušovania ochrany údajov a kybernetických útokov, ale aj ochrany digitálnej identity pred krádežou totožnosti alebo manipuláciou;

²¹ Tamže, bod 3.1.

²² Bližšie pozri tamže, bod 3.2.

²³ Bližšie pozri ANDRAŠKO, J. – MESARČÍK, M. – SOKOL, P. Právo kybernetickej bezpečnosti. Učebnica. Univerzita Komenského v Bratislave, Právnická fakulta, 2022, 2. kapitola.

²⁴ Európska Komisia. Európske vyhlásenie o digitálnych právach a zásadách v digitálnom desaťročí. COM(2022) 28 final. Dostupné na: <https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles>.

²⁵ Tamže, s. 5.

2. bojovať proti tým, ktorí sa snažia oslabiť bezpečnosť a integritu online prostredia Európanov alebo propagovať násilie a nenávisť digitálnymi prostriedkami, a postihovať ich.²⁶

Máme za to, že prvý cieľ napĺňa primárne legislatíva v oblasti kybernetickej bezpečnosti (Smernica NIS), ochrany osobných údajov (GDPR, ePrivacy smernica) a elektronickej identifikácie (Nariadenie eIDAS). Druhý cieľ má skôr medzinárodný charakter, ale zároveň na problematiku hybridných hrozieb reaguje aj regulácie kybernetickej bezpečnosti alebo digitálnych služieb.

Úloha pre MIRRI

Monitorovať proces prijatia Európskeho vyhlásenia o digitálnych právach a zásadách v digitálnom desaťročí s ohľadom na záväzky v oblasti kybernetickej bezpečnosti.

2.2.1. Ochrana osobných údajov

Na úrovni Európskej únie bola viac ako 20 rokov v platnosti smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Nakoľko však išlo o smernicu, členské štáty si povinnosti uvedené v nej implementovali do svojich národných právnych poriadkov odlišným spôsobom.

Od roku 2012 prebiehali odborné diskusie a debaty v rámci európskych štruktúr týkajúcich sa modernizácie daného právneho rámca. Výsledkom spoločnej snahy viacerých aktérov bolo prijatie nového legislatívneho rámca regulujúceho ochranu osobných údajov v podobe nariadenia 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 alebo GDPR); a tzv. Policajnej smernice.

Zároveň je potrebné dodať, že GDPR v určitých otázkach ponechalo voľnosť pre členské štáty a tie a tak v národných právnych poriadkoch mohli upraviť napr. vyváženie práva na ochranu osobných údajov a slobodu prejavu či právo na informácie, otázky mlčanlivosti, vek maloletých pri používaní služieb informačnej spoločnosti či ďalšie otázky. Otázky bezpečnosti ale v rámci týchto tzv. „otvorených klauzúl“ nefigurujú a bude sa tak na nich vzťahovať všeobecná právna úprava v podobe GDPR.

2.2.1.1. Pôsobnosť GDPR

Vecná pôsobnosť GDPR je upravená v článku 2 ods. 1 GDPR. Daný článok upravuje pozitívnu vecnú pôsobnosť GDPR. V zmysle dikcie predmetného článku sa GDPR aplikuje na spracúvanie osobných údajov, ktoré je vykonávané (i) automatizovanými prostriedkami, (ii) čiastočne automatizovanými prostriedkami alebo (iii) manuálne, ak osobné údaje tvoria súčasť informačného systému.

²⁶ Tamže.

Samotné spracúvanie osobných údajov je definované v článku 4 bode 2 GDPR, a to demonštratívnymi výpočtom spracovateľských operácií, ktoré možno subsumovať pod definíciu spracúvania osobných údajov. V zmysle daného článku sa pod spracúvaním osobných údajov rozumie: „operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.“ V zásade možno zhrnúť, že z hľadiska vecnej pôsobnosti sa GDPR bude vzťahovať aj na automatizované spracúvanie v rámci bezpečnostných aktivít ako napríklad detekcia potenciálnych hrozieb alebo monitorovanie siete.

Ústredným pojmom GDPR je však definícia osobného údaje. Osobným údajom „je akékoľvek informácia týkajúca sa identifikovanej alebo identifikovateľnej fyzickej osoby.“²⁷ Identifikovateľná fyzická osoba je taká osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä prostredníctvom odkazu na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Pojem identifikovateľnosti ďalej vykladá recitál 26 GDPR.²⁸ Tento recitál reprezentuje tzv. test primeranej pravdepodobnosti, ktorý odpovedá na to, či konkrétna dotknutá osoba je skutočne identifikovateľná. Predmetným testom sa zaoberal aj Súdny dvor Európskej únie v prípade *Patrick Breyer v Spolková republika Nemecko*. Skutkovo sa prípad týkal otázky, či dynamická IP adresa predstavuje osobný údaj v zmysle staršej legislatívy na ochranu osobných údajov. Prevádzkovateľ webového sídla mal k dispozícii IP adresa užívateľa, avšak nemal priamo informáciu, na koho je táto IP adresa registrovaná. Tieto informácie má zvyčajne k dispozícii poskytovateľ internetového pripojenia. Otázka teda bola, či pre prevádzkovateľa webového sídla predstavuje IP adresa osobný údaj v zmysle legálnej definície. Luxemburský súd judikoval: „...že dynamická IP adresa, ktorú poskytovateľ online mediálnych služieb uchováva v súvislosti s prehliadaním si určitou osobou internetovej stránky, ktorú tento poskytovateľ sprístupnil verejnosti, predstavuje pre tohto poskytovateľa osobný údaj v zmysle tohto ustanovenia, ak má k dispozícii právne prostriedky, na základe ktorých dokáže identifikovať dotknutú osobu vďaka ďalším informáciám, ktorými disponuje poskytovateľ internetového pripojenia tejto osoby.“²⁹ Toto rozhodnutie tak znamená, že ak existujú právom dovolené prostriedky na identifikáciu jednotlivca, pôjde o osobné údaje. Možno dôvodne predpokladať, že aj údaje spracúvané v rámci preventívnych alebo reaktívnych technických a organizačných opatrení na zabezpečenie kybernetickej bezpečnosti možno subsumovať pod legálnu definíciu pojmu osobné údaje. K pojmu osobný údaj teda možno záverom dodať, že nie

²⁷ GDPR, článok 4 bod 1.

²⁸ „Na určenie toho, či je fyzická osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, pri ktorých existuje primeraná pravdepodobnosť, že ich prevádzkovateľ alebo akákoľvek iná osoba využije, napríklad osobitným výberom, na priamu alebo nepriamu identifikáciu fyzickej osoby. Na zistenie toho, či je primerane pravdepodobné, že sa prostriedky použijú na identifikáciu fyzickej osoby, by sa mali zohľadniť všetky objektívne faktory, ako sú náklady a čas potrebný na identifikáciu so zreteľom na technológiu dostupnú v čase spracúvania, ako aj na technologický vývoj.“

²⁹ Rozhodnutie Súdneho dvora Európskej únie, C-582/14 Patrick Breyer proti Bundesrepublik Deutschland.

každá informácia je automaticky osobným údajom. Vždy bude záležať od konkrétnych okolností a kontextu, či je daná osoba identifikovateľná alebo nie.

GDPR upravuje v článku 2 ods. 2 negatívnu pôsobnosť nariadenia. To znamená situácie, keď sa GDPR neaplikuje. Ide predovšetkým o situácie, na ktoré sa neaplikuje právo Európskej únie, otázky národnej bezpečnosti a tajných služieb či otázky patriace do pôsobnosti Policajnej smernice. Osobitne zaujímavou otázkou je výnimka z pôsobnosti, ktorá sa aplikuje v prípade, že spracúvanie osobných údajov prebieha fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti.³⁰ GDPR však nedefinuje, o aké situácie konkrétne ide. Judikatúra SDEÚ však naznačuje určitý smer, kedy sa GDPR vzhľadom na negatívnu pôsobnosť nevzťahuje. O spracúvanie v rámci výlučne osobnej alebo domácej činnosti nepôjde vtedy, ak sú osobné údaje zverejnené na internete³¹ prípadne monitorovanie ulice kamerovým systémom umiestneným nad dverami domu.³²

GDPR upravuje územnú pôsobnosť v rámci článku 3. Je faktom, že nariadenie sa aplikuje v rámci spracúvania osobných údajov v prevádzke, ktorá má sídlo v EÚ (tzv. intra-teritoriálny režim), ale zároveň aj na prevádzkovateľov, ktorí majú sídlo mimo EÚ (tzv. extra-teritoriálny režim) za predpokladu, že ponúkajú osobám v EÚ tovary a služby alebo sledujú ich správanie napríklad prostredníctvom webovej aktivity.

Z hľadiska osobnej pôsobnosti je potrebné rozlišovať 5 typov entít v zmysle GDPR. Najdôležitejšími pojmami sú dotknutá osoba, prevádzkovateľ a sprostredkovateľ. Pre kompletnosť uvádzame aj definíciu pojmov príjemcov a tretej strany.

Dotknutá osoba znamená identifikovanú alebo identifikovateľnú osobu, ktorej sa osobné údaje týkajú. GDPR nedefinuje termín dotknutá osoba, ale jej vymedzenie možno odvodiť z ustanovení týkajúcich sa pojmu osobný údaj (článok 4 bod 1 GDPR).

Prevádzkovateľ³³ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov, pričom platí, že ak sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu. Najdôležitejším aspektom definície prevádzkovateľa je „určenie účelu.“ Entita, ktorá určí účel spracúvania osobných údajov (dôvod, prečo sú osobné údaje spracúvané) je prevádzkovateľom. Prevádzkovateľom tak môže byť napríklad orgán verejnej moci, ktorý spracúva údaje vo svojej sieti alebo v rámci bezpečnostných opatrení. Za prevádzkovateľov možno považovať aj prevádzkovateľov základných služieb, poskytovateľov digitálnych služieb a súvisiace entity podľa ZoITVS. Spoloční prevádzkovatelia³⁴ sú dvaja alebo viacerí prevádzkovatelia, ktorí spoločne určujú účely a prostriedky spracúvania. Ak dvaja alebo viacerí prevádzkovatelia spoločne určujú účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.

³⁰ GDPR, článok 2 ods. 2 písm. c).

³¹ Rozhodnutie Súdneho dvora Európskej únie, C-101/01- Lindqvist.

³² Rozhodnutie Súdneho dvora Európskej únie, C-212/13-Ryneš.

³³ GDPR, článok 4 bod 7.

³⁴ GDPR, článok 26 ods. 1.

Sprostredkovateľ³⁵ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa. To znamená, že v tomto prípade je nevyhnutné mať poverenie a pokyny od prevádzkovateľa ako spracúvať osobné údaje v jeho mene. Nie je vylúčené, že jedná entita môže figurovať aj ako prevádzkovateľ a aj ako sprostredkovateľ.

Príjemca³⁶ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je tretou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov. Tretia strana³⁷ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.

2.2.1.2. Kybernetická bezpečnosť

Spracúvanie osobných údajov a otázky kybernetickej bezpečnosti nie je možné vnímať oddelene. Vyplyva to aj z typického konfliktu medzi ochranou súkromia a zabezpečením bezpečnosti, kde jedno nie je možné vykonať bez narušenia druhého. Na jednej strane, spracúvanie údajov na účely bezpečnosti môže byť vnímané ako invazívny zásah do súkromia. Na strane druhej, ak by sme dáta užívateľov nespracúvali, mohlo by dôjsť k neželaným následkom z hľadiska bezpečnosti.

Samotnú bezpečnosť rámčuje zásada integrity a dôvernosti: *„Osobné údaje musia byť... spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).*³⁸

Bezpečnosť a jej požiadavky v zmysle spracúvania osobných údajov sú upravené v článku 32 GDPR. Práve tento článok nadväzuje už na spomínanú zásadu integrity a dôvernosti uvedenú vyššie, ktoré reflektujú bezpečnostné požiadavky na spracúvanie osobných údajov.

Článok 32 ods. 1 upravuje všeobecnú klauzulu bezpečnosti: *„Prevádzkovateľ a sprostredkovateľ prijímú so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku...“* Diskutovaný článok explicitne ustanovuje požiadavky triády kybernetickej bezpečnosti (CIA) uvedené v úvode tejto učebnice. Zachováva tak konzistentnosť požiadaviek na kybernetickú bezpečnosť v rámci právnych rámcov. Zároveň daný článok vymedzuje demonštratívny výpočet bezpečnostných opatrení, ktoré môže prevádzkovateľ alebo sprostredkovateľ prijať. Konkrétne:

- pseudonymizáciu a šifrovanie osobných údajov;

³⁵ GDPR, článok 4 bod 8.

³⁶ GDPR, článok 4 bod 9.

³⁷ GDPR, článok 4 bod 10.

³⁸ GDPR, článok 5 ods. 1 písm. f).

- schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
- schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
- proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Článok 32 opakovane zdôrazňuje požiadavku primeranosti bezpečnostných opatrení. Prakticky to znamená, že prevádzkovatelia a sprostredkovatelia musia identifikovať konkrétne riziká v konkrétnych situáciách a zohľadniť špecifiká spracúvania osobných údajov ako napr. citlivosť údajov prípadne ďalší kontext. „Pri posudzovaní primeranej úrovne bezpečnosti sa prihliada predovšetkým na riziká, ktoré predstavuje spracúvanie, a to najmä v dôsledku náhodného alebo nezákonného zničenia, straty, zmeny, neoprávneného poskytnutia osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávneného prístupu k takýmto údajom.“ Samotná referencia na primeranosť znamená aj úzke prepojenie na princíp proporcionality, ktorý je všeobecne známy a preferovaný v práve EÚ. Proportionality vo všeobecnosti znamená, že je potrebné merať vhodnosť použitých prostriedkov vzhľadom na účel a úmysel dosiahnutia výsledkov.

Úloha pre MIRRI

Pri komunikovaní usmernení a odporúčaní pre bezpečnostné opatrenia v zmysle ZoKB alebo ZoITVS je potrebné upriamiť pozornosť aj na otázky článku 32 GDPR. Považujeme to za nevyhnutné, aby adresáti usmernení alebo odporúčaní mali komplexný obraz o regulácii bezpečnosti.

Druhou zložkou bezpečnosti v rámci GDPR je problematika nahlasovania porušení ochrany osobných údajov. Porušenie ochrany osobných údajov je definované v článku 4 bode 12 GDPR nasledovne: „porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.“

Vzhľadom na atribúty informácie v zmysle teórie informačnej bezpečnosti možno porušenia ochrany osobných údajov rozdeliť na:

- Porušenie dôvernosti (*confidentiality breach*) napr. únik osobných údajov;
- Porušenie integrity (*integrity breach*) napr. kompromitovanie kamerového záznamu; a
- Porušenie dostupnosti (*availability breach*) napr. hacknutie systému a odopretie prístupu k osobným údajom povereným osobám.³⁹

Samotné nahlasovanie (reportovanie) porušení ochrany osobných údajov môžeme deliť podľa entity, ktorej sa tieto incidenty nahlasujú. Článok 33 GDPR upravuje nahlasovanie porušení ochrany

³⁹ K tomu pozri aj Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

osobných údajov **dozornému orgánu** a článok 34 GDPR upravuje nahlasovanie porušení ochrany osobných údajov **dotknutej osobe**.

*„V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr **do 72 hodín** po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55 s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb. Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.“* (Článok 33 GDPR)

*„V prípade porušenia ochrany osobných údajov, ktoré **pravdepodobne povedie k vysokému riziku** pre práva a slobody fyzických osôb, prevádzkovateľ **bez zbytočného odkladu** oznámi porušenie ochrany osobných údajov dotknutej osobe.“* (Článok 34 GDPR).

Najdôležitejšiu časť analýzy tvorí posúdenie, či predmetné porušenie vedie **k (vysokým) rizikám pre práva a slobody dotknutých osôb**.

Ak je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb, prevádzkovateľ je povinný do 72 hodín od momentu zistenia („po tom, čo sa o tom prevádzkovateľ dozvedel“) incident nahlásiť **dozornému orgánu**. Nie je tak potrebné nahlasovať incidenty, ktoré nepredstavujú riziká pre práva a slobody fyzických osôb.

V prípade, ak sa porušenie ochrany osobných údajov stane na strane sprostredkovateľa, je o tom povinný informovať prevádzkovateľa bez zbytočného odkladu.⁴⁰ Pri komplexnejších situáciách je možné dozorný orgán informovať postupne s vysvetlením, prečo tak prevádzkovateľ robí. Úrad na ochranu osobných údajov Slovenskej republiky má na svojom webe zverejnený formulár, prostredníctvom ktorého je možné porušenia ochrany osobných údajov nahlasovať.⁴¹ Následne je prevádzkovateľ povinný predmetný incident zdokumentovať.

O porušení ochrany osobných údajov je potrebné informovať **dotknuté osoby** za predpokladu, že toto porušenie pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb. V takom prípade je prevádzkovateľ povinný túto informáciu poskytnúť dotknutým osobám bezodkladne.⁴² Kritéria na posúdenie vysokého rizika vymedzila Pracovná skupina čl. 29 vo svojom usmernení.⁴³ Konkrétne ide o

- typ porušenia;
- povaha, citlivosť a kvantita údajov;
- možnosť identifikácie jednotlivcov;
- závažnosť dopadu pre jednotlivcov;
- či ide o dáta detí a zraniteľné osoby;
- rola prevádzkovateľa;
- počet zasiahnutých osôb prípadne ďalšie faktory.⁴⁴

⁴⁰ Vid' GDPR, článok 33 ods. 2.

⁴¹ <https://dataprotection.gov.sk/uoou/sk/dp/dp-breach> (dostupné 12.8.2021).

⁴² GDPR, článok 34 ods. 1.

⁴³ Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01.

⁴⁴ Tamže.

Ako príklad hodnotenia rizika pri porušení ochrany osobných údajov je možné uviesť nasledovné: Nemocnica v krajskom meste sa stane obeťou kybernetického útoku, pri ktorom sú kompromitované údaje zamestnancov a pacientov. Údaje sú riadne zálohované a šifrované. Vyšetrovanie ukáže, že útočník osobné údaje iba videl, ale nestiahol si ich. Záloha údajov a nastavenie systémov do pôvodnej prevádzky ale trvalo dva dni, počas ktorých bolo limitované poskytovanie zdravotnej starostlivosti. Napriek tomu, že nedošlo ku veľkej škode čo sa týka samotných osobných údajov, činnosť nemocnica bola obmedzená a z toho dôvodu by mal byť tento prípad klasifikovaný ako nesúci vysoké riziko.

V prípade, ak prevádzkovateľ vysoké riziko pri porušení ochrany osobných údajov vyhodnotí, nemusí automaticky dotknuté osoby informovať. GDPR totiž ustanovuje tri výnimky, keď prevádzkovateľ takéto incidenty nemusí notifikovať dotknutým osobám. Prvou výnimkou sú prípady, ak prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie.⁴⁵ Druhým prípadom je situácia, ak prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky.⁴⁶ Poslednou výnimkou je prípad, ak by si informovanie vyžadovalo neprimerané úsilie. V takom prípade však dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.⁴⁷ Ak prevádzkovateľ túto povinnosť nesplní, dozorný orgán si môže notifikačnú povinnosť vynútiť.⁴⁸ Aj v tomto prípade je prevádzkovateľ povinný predmetný incident zdokumentovať.

Úloha pre MIRRI

Nahlasovanie bezpečnostných incidentov a ich modalít je predmetom právnej úpravy viacerých aktov. Menovať môžeme GDPR, zákon o elektronických komunikáciách, ZoKB, ZoITVS, zákon o platbách či Nariadenie eIDAS. Je preto viac ako pravdepodobné, že jedna entita bude musieť nahlasovať bezpečnostné incidenty podľa rôznych právnych predpisov.

Z pohľadu MIRRI je preto dôležité čo najviac vplývať na úpravu legislatívy tak, aby nahlasovanie bezpečnostných incidentov podľa rôznych právnych predpisov bolo uchopené koncepčne a pokiaľ možné aj jednotne. Minimom by malo byť vzdelávanie a konkrétne odporúčania s metodikami pre nahlasovanie bezpečnostných incidentov pre adresátov noriem v pôsobnosti MIRRI.

V kontexte bezpečnosti a GDPR považujeme za potrebné upriamiť pozornosť aj na inštitút zodpovednej osoby (Data Protection Officer, **DPO**). Zodpovedná osoba musí mať nezávislé postavenie pri plnení svojich úloh. To prakticky znamená, že prevádzkovateľ alebo sprostredkovateľ je povinný

⁴⁵ GDPR, článok 34 ods. 3 a).

⁴⁶ GDPR, článok 34 ods. 3 b).

⁴⁷ GDPR, článok 34 ods. 3 c).

⁴⁸ Vid' GDPR, článok 34 ods. 4.

zabezpečiť, aby zodpovedná osoba v súvislosti s plnením týchto úloh nedostávala žiadne pokyny. Zároveň zodpovednú osobu nesmú odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba podlieha priamo najvyššiemu vedeniu prevádzkovateľa alebo sprostredkovateľa.⁴⁹ Z hľadiska úloh upravených v článku 39 GDPR možno povinnosti zodpovednej osoby rozdeliť do štyroch oblastí:

- **monitorovanie** – zodpovedná osoba monitoruje súlad s GDPR a inými právnymi predpismi v danej organizácii vrátane interných predpisov a taktiež vykonáva interné audity;
- **poradenstvo** – zodpovedná osoba poskytuje na požiadanie poradenskú činnosť v oblasti ochrany osobných údajov organizácií a jej zamestnancom; osobitne možno zdôrazniť poradenskú činnosť pri vypracovaní posúdenia vplyvu na ochranu osobných údajov v zmysle článku 35 GDPR;
- **vzdelávanie** – zodpovedná osoba obstaráva vzdelávanie zamestnancov organizácie, školí ich v danej oblasti a zvyšuje povedomie a odbornosť v danej oblasti;
- **kontaktný bod** – zodpovedná osoba plní úlohu kontaktného miesta pre dotknuté osoby pri výkone ich práv a pre dozorný orgán pri spolupráci alebo predchádzajúcej konzultácii.

Kedy je prevádzkovateľ alebo sprostredkovateľ povinný dotknutú osobu vymenovať, upravuje článok 37 ods. 1 GDPR. V zmysle daných ustanovení táto povinnosť nastáva, ak:

- **spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt** s výnimkou súdov pri výkone ich súdnej právomoci;
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu alebo
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov podľa článku 9 GDPR vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10 GDPR.

Hlavnou činnosťou v zmysle vyššie uvedených ustanovení sa myslí taká činnosť, ktorá je absolútne rozhodujúca pre činnosť danej organizácie.

Úloha pre MIRRI

Rola DPO je významne previazaná s úlohami manažéra kybernetickej bezpečnosti. Z tohto dôvodu považujeme za nevyhnutné, aby MIRRI v rámci vzdelávania v oblasti kybernetickej bezpečnosti zahrnula aj oblasť ochrany osobných údajov. Uvedené je potrebné integrovať aj v rámci metodických usmernení pre orgány verejnej moci z hľadiska bezpečnosti.

⁴⁹ GDPR, článok 38 ods. 3.

2.2.2. Umeľá inteligencia

Európska komisia v apríli 2021 po niekoľko-mesačných snahách predstavila prvý komplexný návrh regulácie umelej inteligencie na svete. Nadviazala tak na dlhoročnú prácu expertných skupín a požiadaviek orgánov Európskej únie v podobe stanovísk či odporúčaní.

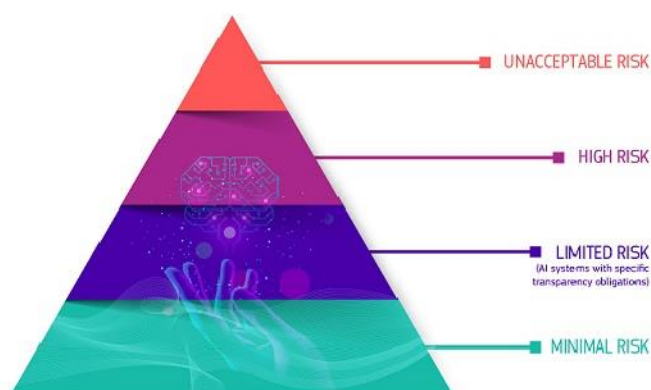
V prvom rade je potrebné zvýrazniť, že AIA je formulovaná skôr ako produktová regulácia a porovnať to možno s požiadavkami na produkty ako napríklad zdravotnícke pomôcky alebo elektronické výrobky pri uvedení na trh. To znamená, že určuje špecifikácie systémov AI, ktoré musia byť splnené pri uvedení na trh a veľkú zodpovednosť ponecháva na samotných prevádzkovateľoch týchto systémov prostredníctvom inštitútu posúdenia zhody (conformity assessment).⁵⁰

2.2.2.1. Pôsobnosť

Prirodzene, kľúčovou definíciou regulácie je pojem systémy AI. Ten je definovaný ako: „*softvér vyvinutý s jednou alebo viacerými technikami a prístupmi uvedenými v prílohe I, ktorý môže pre daný súbor cieľov vymedzených človekom vytvárať výstupy, ako je obsah, predpovede, odporúčania alebo rozhodnutia ovplyvňujúce prostredie, s ktorým sú v interakcii.*“⁵¹ Príloha I následne uvádza konkrétne techniky spadajúce pod pojem AI. Predmetná definícia je rozsiahlo kritizovaná technologickým sektorom, ale aj akademickou obcou pre svoju všeobecnosť a extenzívnosť a je pravdepodobné, že bude ešte v revíziách návrhu upravená.

AIA je horizontálna regulácia založená na skúmaní rizika. To prakticky znamená, že vymedzuje systémy AI v kontexte rôznych typov rizík pre základné ľudské práva a slobody⁵² a následne upravuje špecifické právne požiadavky pre tieto systémy v danej kategórii. AIA v zásade rozlišuje:

- Neakceptovateľné riziko (zakázané praktiky);⁵³



Obrázok: Systémy AI podľa rizika.
Zdroj: Web Európskej komisie.

⁵⁰ Základ pre vypracovanie tejto state tvorí MESARČÍK, M. Automatizované rozhodovanie vo verejnej správe vo svetle novej právnej úpravy. In HAVELKOVÁ, M. – JAKUŠOVÁ, V. (ed). Aktuálne otázky digitálneho trhu Európskej únie vo verejnom sektore. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2021.

⁵¹ AIA, článok 3 ods. 1.

⁵² Napríklad AIA, recitál 15: „*Využívanie umelej inteligencie má síce mnoho výhod, túto technológiu však možno zneužiť a môže sa stať zdrojom nových a výkonných nástrojov umožňujúcich manipulatívne a zneužívajúce praktiky a praktiky v oblasti sociálnej kontroly. Takéto praktiky sú mimoriadne škodlivé a mali by sa zakázať, pretože sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv Únie vrátane práva na nediskrimináciu, ochranu údajov a súkromia a práv dieťaťa.*“

⁵³ AIA, článok 5. Konkrétne sú zakázané praktiky ako zavádzanie a používanie systémov AI, ktorý s cieľom podstatne narušiť správanie osoby využíva podprahové techniky mimo vedomia osoby tak, že tejto alebo inej osobe spôsobí alebo by mohol spôsobiť fyzickú alebo psychickú ujmu; uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému umelej inteligencie, ktorý s cieľom podstatne narušiť správanie osoby patriacej do konkrétnej skupiny osôb využíva ktorúkoľvek zo zraniteľností tejto skupiny osôb vyplývajúcich z ich veku, fyzického alebo duševného postihnutia tak, že tejto alebo inej osobe spôsobí alebo by mohol

- Vysoké riziko
- Nízke riziko
- Žiadne riziko.

AIA sa automaticky nevzťahuje na všetky systémy AI v zmysle definície uvedenej vyššie. AIA sa bude aplikovať na systémy AI, ktoré sú súčasťou produktu v rámci špecifickej produktovej právnej úpravy⁵⁴ (napr. hračiek, výťahov alebo medicínskych pomôcok). Ak je AI súčasťou alebo samostatným produktom pri niektorej z uvedených produktových regulácií, vzťahuje sa na nich kľúčová časť 3 AIA, ktorá obsahuje drvivú väčšinu povinností pre systémy AI.

Ak systém AI nespadá pod osobitnú reguláciu, prevádzkovatelia sa musia pozrieť na prílohu III AIA, ktorá ustanovuje oblasti AI vysokého rizika, na ktoré sa následne právny akt vrátane kľúčovej tretej časti aplikuje. Konkrétne ide o oblasti:

- Biometrická identifikácia a kategorizácia fyzických osôb;
- Riadenie a prevádzka kritickej infraštruktúry;
- Vzdelávanie a odborná príprava;
- Zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti;
- Prístup k základným súkromným a verejným službám a dávkam a ich využívanie;
- Presadzovanie práva;
- Migrácia, azyl a riadenie kontroly hraníc; a
- Výkon spravodlivosti a demokratické procesy.

Každá z vyššie uvedených oblastí je následne v Prílohe III charakterizovaná prostredníctvom viacerých konkrétnych aplikácií. Napríklad, oblasť spravodlivosti a demokratických procesov zahŕňa: „*systémy umelej inteligencie určené na pomoc súdnemu orgánu pri skúmaní a interpretácii faktov a práva a pri uplatňovaní práva na konkrétny súbor skutočností.*“⁵⁵

Z vyššie uvedeného je zjavné, že AIA bude výrazne regulovať využívanie systémov AI aj vo verejnom sektore. Zvýrazňujeme hlavne oblasť riadenia a prevádzky kritickej infraštruktúry, prístupu k verejným službám či výkonu spravodlivosti. V poslednom verejne dostupnom kompromisnom znení bola výslovne pridaná aj oblasť „**digitálnej infraštruktúry.**“⁵⁶

Úloha pre MIRRI

Monitorovať proces prijatia aktu o umelej inteligencii a vyhodnocovať vplyv nariadenia na využívanie systémov AI v kritickej infraštruktúre a digitálnej infraštruktúre.

spôsobiť fyzickú alebo psychickú ujmu; tzv. kreditný skóring orgánov verejnej moci s dôsledkom škodlivého alebo nepriaznivého zaobchádzania. Zároveň AIA výrazne limituje využívanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva. Pozri viac v Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach." *Computer Law Review International* 22.4 (2021): 97-112.

⁵⁴ Tieto výslovne AIA menuje v prílohe č. 2.

⁵⁵ AIA, Príloha III, bod 8 písm. a).

⁵⁶ Dostupné na: <https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf>.

Takmer vôbec sa regulácia netýka systémov AI nízkeho resp. minimálneho rizika, kde ustanovuje iba strohé požiadavky na transparentnosť a odporúčanie prijatia kódexov správania, ktoré výrobcovia a prevádzkovatelia takýchto AI systémov budú dodržiavať.

Z hľadiska negatívnej pôsobnosti sa AIA nevzťahuje na systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské účely a na produkty v rámci právnych aktov výslovne vymenovaných v článku 2 ods. 2 AIA ako napr. nariadenie o bezpečnostnej ochrany civilného letectva alebo nariadenie o schvaľovaní motorových vozidiel.

Drvivá väčšina požiadaviek v AIA sa zameriava na regulácie systémov AI vysokého rizika. Ak bude chcieť výrobca uviesť vysoko-rizikový systém AI na trh a následne do praxe, bude musieť v zmysle požiadaviek AIA splniť niekoľko krokov. Je nutné poznamenať, že AIA dáva obrovský dôraz na splnenie požiadaviek pred uvedením na trh (*ex ante*), aby sa minimalizovali riziká AI z hľadiska bezpečnosti a rešpektovania základných ľudských práv pri jej používaní.

Prvým krokom je vykonanie tzv. posudzovania zhody (*conformity assessment*), čo je proces známy aj z iných regulácií. Jeho zmyslom je, aby výrobca systémov AI sám dbal na dodržiavanie požiadaviek AIA, ktoré mu nariadenie ustanovuje. Ako príklady možno uviesť požiadavky na správnosť a reprezentatívnosť údajov, ktoré umelá inteligencia spracúva či nutnosť procesov na zisťovanie potenciálnych skreslení (predsudkov).⁵⁷ Ďalšie požiadavky sa týkajú vyhotovenia technickej dokumentácie⁵⁸ či transparentnosti v podobe informovania užívateľov (právnických osôb).⁵⁹

Zaujímavosťou možno je, že tieto posudzovania zhody si vo veľkej miere môžu manažovať vývojári systémov AI vo vlastnej réžií. Výnimku predstavujú iba veľmi špecifické aplikácie ako napríklad použitie vzdialenej biometrie, kde v takom prípade posúdenie zhody vykonáva notifikovaná osoba akreditovaná národným notifikačným orgánom.

Druhým krokom po úspešnom posúdení zhody je registrácia systému AI v databáze EÚ pre samostatné vysokorizikové systémy umelej inteligencie.⁶⁰ Túto databázu bude spravovať samotná Európska komisia spolu s členskými štátmi. Databáza bude verejne dostupná a tak si každý užívateľ môže overiť, či je systém AI registrovaný a prešiel posúdením zhody.

EÚ následne pre registrovaný vysokorizikový AI systém vydá tzv. vyhlásenie o zhode.⁶¹ Zároveň výrobca označenie zhody umiestni tak, aby bolo viditeľné, čitateľné a neodstrániteľné.⁶²

Tretím krokom je *ex post* monitorovanie systémov AI po uvedení na trh. Prakticky to znamená výkon dohľadu a monitorovania vysokorizikových systémov AI. Po vzore iných právnych úprav je zakotvený inštitút nahlasovania incidentov pri využívaní systémov AI.⁶³

Samotný dozor budú vykonávať príslušné vnútroštátne orgány. V podmienkach slovenskej republiky to znamená, že buď zákonodarca vytvorí nový orgán verejnej moci alebo tieto právomoci prideli už existujúcemu orgánu.

⁵⁷ AIA, článok 10.

⁵⁸ AIA, článok 11.

⁵⁹ AIA, článok 12.

⁶⁰ AIA, článok 60.

⁶¹ AIA, článok 48.

⁶² AIA, článok 49.

⁶³ AIA, článok 62.

AIA sa bude vzťahovať na tie systémy, ktoré budú uvedené na trhu po nadobudnutí účinnosti. Súčasné používané vysokorizikové systémy AI budú musieť spĺňať požiadavky AIA iba v prípade, ak prejdú „zásadnou zmenou,“ pričom tento pojem v regulácii nie je definovaný.⁶⁴ Vytváranie takejto dvojkoľajnosti je predmetom kritiky a tento prístup môže ešte zákonodarca upraviť.

Zaujímavosťou sú aj sankcie za porušenie AIA. Tie sú upravené ešte striktnejšie ako pri GDPR. Za porušenie ustanovení AIA bude možné uložiť pokutu až do výšky 30 000 000 EUR, alebo ak je porušiteľom spoločnosť, až do výšky 6 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia za porušenie zakázaných praktík a nesúlad s požiadavkami na správu údajov. Ďalej AIA umožňuje správne pokuty do výšky 20 000 000 EUR a 10 000 000 EUR.⁶⁵

Dohľad nad dodržiavaním pravidiel pred uvedením systému AI vysokého rizika na trh je určený iba v špecifických prípadoch prostredníctvom akreditovaných orgánov. AIA ustanovuje povinnosť pre členské štáty kreovať alebo určiť dozorný orgán, ktorý bude vykonávať štátny dozor. Na úrovni EÚ zároveň vznikne Európska rada pre umelú inteligenciu.

2.2.2.2. Kybernetická bezpečnosť

Vzťah AIA a kybernetickej bezpečnosti najlepšie reflektuje recitál 51: *„Kybernetická bezpečnosť zohráva **klúčovú úlohu pri zabezpečovaní odolnosti systémov umelej inteligencie** voči pokusom o zmenu ich použitia, správania, výkonnosti alebo o ohrozenie ich bezpečnostných vlastností tretími stranami, ktoré so škodlivým úmyslom zneužívajú zraniteľné miesta systému. **Kybernetické útoky na systémy umelej inteligencie môžu využívať aktíva špecifické pre umelú inteligenciu**, ako sú súbory trénovacích údajov (napr. otrávenie údajov) alebo trénované modely (napr. nepriateľské útoky), alebo zneužívať zraniteľné miesta digitálnych aktív systému umelej inteligencie alebo základnej infraštruktúry IKT. **Na zabezpečenie úrovne kybernetickej bezpečnosti primeranej rizikám by preto poskytovatelia vysokorizikových systémov umelej inteligencie mali prijať vhodné opatrenia a náležite pritom zohľadniť základnú infraštruktúru IKT.**“*

Z vyššie uvedenej všeobecnej deklarácie následne vyplývajú konkrétne požiadavky na zabezpečenie kybernetickej bezpečnosti pre vysokorizikové systémy AI. Predmetné požiadavky sú legislatívne zhmotnené v článku 15 AIA, v zmysle ktorého vysokorizikové systémy AI musia byť **odolné voči pokusom neoprávnených tretích strán o zmenu ich používania alebo výkonnosti využívaním zraniteľností systému**. Zároveň AIA vyžaduje, aby technické riešenia zamerané na zabezpečenie kybernetickej bezpečnosti vysokorizikových systémov umelej inteligencie musia byť primerané príslušným okolnostiam a rizikám.

Špecificky, článok 15 ods. 4 vyžaduje presné opatrenia v kontexte trénovacích dát: *„Technické riešenia na riešenie zraniteľností špecifických pre umelú inteligenciu musia v prípade potreby zahŕňať opatrenia na prevenciu a kontrolu útokov, ktoré sa pokúšajú manipulovať súbor trénovacích údajov*

⁶⁴ AIA, článok 83.

⁶⁵ AIA, článok 71.

(„otrávenie údajov“), vstupov upravených tak, aby model urobil chybu („odporujúce si príklady“), alebo nedostatkov modelu.“ Všetky požiadavky uvedené v článku 15 AIA musia byť transparentne komunikované užívateľom, ktorými sú v zmysle AIA primárne business používatelia systémov AI. Presnejšie označenie pre túto skupinu by boli nasadzovatelia („deployers“).

Ak vysokorizikový systém AI získa certifikáciu alebo vyhlásenie o zhode podľa Aktu o kybernetickej bezpečnosti, požiadavky na kybernetickú bezpečnosť podľa článku 15 sa považujú za splnené.⁶⁶

Úloha pre MIRRI

Monitorovať prijímanie štandardov v zmysle Aktu o kybernetickej bezpečnosti pre systémy AI.

Dôležitú úlohu v rámci kybernetickej bezpečnosti zohráva štandardizácia t. j. tvorba štandardov pre kybernetickú bezpečnosť vrátane prijímania a akceptovania pravidiel samotným trhom (mimo štátnych aktérov). Podobne, AIA explicitne ráta s významnou rolou štandardov v rámci vypracovania posudzovania zhody: „Vysokorizikové systémy umelej inteligencie, ktoré sú v **zhode s harmonizovanými normami alebo ich časťami**, na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie, sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v kapitole 2 tejto hlavy, pokiaľ sa uvedené normy na tieto požiadavky vzťahujú.“⁶⁷ Momentálne v EÚ pôsobia tri štandardizačné organizácie, pričom z interných diskusií a prezentácií vypláva, že Európska komisia sa bude primárne opierať o štandardy CEN (*European Committee for Standardisation*) a CENELEC (*European Committee for Electrotechnical Standardisation*).⁶⁸ Prakticky, ak prevádzkovatelia vysokorizikových systémov AI budú rešpektovať dané štandardy, platí prezumpcia zhody s požiadavkami AIA. Platí, že pre prevádzkovateľov je jednoduchšie tieto štandardy prevziať, nakoľko sú častokrát špecifickejšie ako legislatívne požiadavky obsahujúce určitú mieru všeobecnosti.⁶⁹ Prirodzene, outsourcing požiadaviek na súkromné entity je kontroverzný a kritizovaný. Hlavným problematickým bodom je otázka preskúmateľnosti takýchto aktov súdnymi orgánmi EÚ.⁷⁰ Štandardy tak teoreticky nemusia naplňať ochranu základných hodnôt a práv, na ktorých je AIA postavená, čo môže predstavovať zásadný problém z pohľadu základných ľudských práv a slobôd.

⁶⁶ AIA, článok 42 ods. 2. „Vysokorizikové systémy umelej inteligencie, pre ktoré bol v rámci systému kybernetickej bezpečnosti podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 vydaný certifikát alebo vyhlásenie o zhode a na ktoré boli uverejnené odkazy v Úradnom vestníku Európskej únie, sa považujú za systémy, ktoré sú v súlade s kyberneticko-bezpečnostnými požiadavkami stanovenými v článku 15 tohto nariadenia, pokiaľ sa certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode alebo ich časti na tieto požiadavky vzťahujú.“

⁶⁷ AIA, článok 40.

⁶⁸ Pozri viac v Veale, Michael, and Frederik Zuiderveen Borgesius. "Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach." *Computer Law Review International* 22.4 (2021): 104.

⁶⁹ Pozri napríklad Rob van Gestel and Hans-W Micklitz, 'European Integration through Standardization: How Judicial Review is Breaking down the Club House of Private Standardization Bodies' (2013) 50 *Common Market Law Review*, 157.

⁷⁰ Bližšie napríklad Harm Schepel, 'Case C-171/11 Fra.Bo SpA v Deutsche Vereinigung Des Gas- Und Wasserfaches' (2013) 9 *European Review of Contract Law*, 192.

Úloha pre MIRRI

Monitorovať prijímanie štandardov v zmysle AIA za predpokladu, že bude platiť prezumpcia správnosti s požiadavkami v legislatíve.

2.2.3. Sociálne média

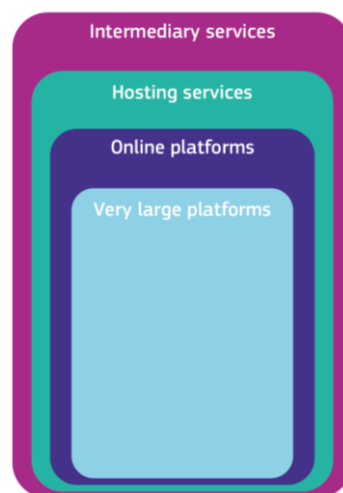
Na sklonku roka 2020 predstavila Európska Komisia návrh nariadenia o digitálnych službách známeho pod skratkou DSA (Digital Services Act). Základným motívom bola revízia dvadsať rokov platného právneho rámca zodpovednosti online platforiem v podobe smernice o elektronickom obchode. Zároveň zákonodarca reflektoval vývoj digitálneho trhu a narastajúcej ekonomickej sily online platforiem, čo podnietilo diskusie o možných rizikách a regulácii. Európska komisia identifikovala niekoľko dôvodov, ktoré viedli k navrhovanej legislatíve. V prvom rade ide o nárast rizík v súvislosti s používaním a správaním online platforiem v podobe sociálnych a ekonomických rizík a novej ujmy pre jednotlivcov a ich základné práva a slobody. Druhým dôvodom je nedostatočný dohľad a spolupráca pri digitálnych službách, čo spôsobuje eróziu jednotného trhu EÚ v kontexte poskytovania digitálnych služieb. Tretím dôvodom je odstránenie bariér pre menšie spoločnosti pri poskytovaní digitálnych služieb vzhľadom na pozíciu veľkých online platforiem.⁷¹ Tieto dôvody sú následne prenesené do konkrétnych požiadaviek v DSA.

2.2.3.1. Pôsobnosť

Návrh DSA z hľadiska osobnej pôsobnosti rozlišuje štyroch aktérov, na ktorých sa vzťahujú konkrétne právne požiadavky. V zásade ide o niekoľko množín vzťahov. DSA rozlišuje:

- Sprostredkovateľské služby;
- Hostingové služby;
- Online platformy; a
- Veľmi veľké online platformy.⁷²

Najväčšou množinou aktérov sú **spostredkovateľské služby**, ktoré návrh DSA delí na služby typu občajný prenos, kešing a hosting.⁷³ Služby typu občajný prenos zahŕňajú



Množiny aktérov v DSA
Zdroj: Webová stránka Európskej Komisia.

⁷¹ Európska Komisia. IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. SWD(2020) 348 final.

⁷² Zdroj obrázku: Európska komisia.

⁷³ DSA, článok 2 písm. f): „spostredkovateľská služba“ je jedna z týchto služieb:

–služba „občajný prenos“, ktorá pozostáva z prenosu informácií poskytovaných príjemcom služby v komunikačnej sieti alebo z poskytovania prístupu ku komunikačnej sieti,

poskytovateľov internetového pripojenia alebo prevádzkovateľov otvorenej wifi siete. Podstatou služieb kešingu je dočasné a prechodné uloženie informácií s cieľom zefektívnenia služby.

Dôležitou množinou z hľadiska šírenia dezinformácií sú služby typu **hosting**. V zásade ide o služby webhostingu, cloudových služieb, úložísk, sociálnych sietí alebo online inzercií. Podmnožinou služieb hosting sú **online platformy**, ktoré DSA definuje ako „poskytovateľ hostingovej služby, ktorý na žiadosť príjemcu služby uchováva a verejne šíri informácie, pokiaľ táto činnosť nie je nevýznamným a čisto vedľajším prvkom inej služby, ktorý z objektívnych a technických dôvodov nemožno použiť bez tejto inej služby, a jeho začlenenie do inej služby nie je prostriedkom na obchádzanie uplatniteľnosti tohto nariadenia.“⁷⁴

Špecifická pozornosť a právne požiadavky sú zamerané aj na poslednú množinu aktérov - **veľmi veľké online platformy**. Tieto priamo definované v DSA nie sú, avšak návrh nariadenia obsahuje návod na klasifikáciu. V zmysle článku 25 ods. 1 DSA veľkými online platformami možno rozumieť tých sprostredkovateľov, „ktorí svoje služby poskytujú priemernému mesačnému počtu aktívnych príjemcov služby v Únii, ktorý sa rovná 45 miliónom alebo je vyšší a ktorý je vypočítaný v súlade s metodikou“ stanovenou v DSA.

Požiadavky kladené DSA na vyššie uvedených aktérov sa líšia a je preto vždy dôležité správne klasifikovať sprostredkovateľa služieb.⁷⁵ Najväčší „balík“ povinností prirodzene prislúcha veľmi veľkým online platformám, ktoré musia spĺňať vyššie požiadavky na transparentnosť, nastavenia odporúčacích systémov, transparentnosti cielenia reklamy či vypracovania krízových protokolov.

2.2.3.2. Kybernetická bezpečnosť

Napriek tomu, že DSA je pomerne špecifická regulácia týkajúca sa hlavne súkromného sektora a digitálnych služieb, obsahuje aj určité čiastkové otázky týkajúce sa kybernetickej bezpečnosti. Osobitne možno tieto povinnosti zvýrazniť pri veľmi veľkých online platformách, ktoré musia prijať viacero opatrení na riešenie tzv. **systémových rizík**. Medzi systémové riziká DSA zaraďuje najmä:

- šírenie nezákonného obsahu prostredníctvom ich služieb;
- akékoľvek negatívne účinky na výkon základných práv na rešpektovanie súkromného a rodinného života, slobody prejavu a práva na informácie, zákazu diskriminácie a práv dieťaťa, ako sú zakotvené v článkoch 7, 11, 21 a 24 charty;
- úmyselná manipulácia ich služieb, a to aj prostredníctvom neautentického používania alebo automatizovaného využívania služby, so skutočným alebo predvídateľným negatívnym vplyvom na ochranu verejného zdravia, maloletých osôb a občianskej diskusie alebo

–služba „**kešing**“, ktorá pozostáva z prenosu informácií poskytovaných príjemcom služby v komunikačnej sieti, pri ktorom sa tieto informácie automaticky, dočasne a prechodne uchovávajú, a to výlučne na účely zefektívnenia ďalšieho prenosu informácií k iným príjemcom na ich žiadosť,

–služba „**hosting**“, ktorá pozostáva z uchovávaní informácií poskytovaných príjemcom služby na jeho žiadosť.“

⁷⁴ DSA, článok 2 písm. h).

⁷⁵ Pozri Európska komisia: Digital Services Act. Dostupné na: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

skutočnými alebo predvídateľnými účinkami súvisiacimi s volebnými procesmi a **verejnou bezpečnosťou**.⁷⁶

Ako konkrétne opatrenia na zmierňovanie systémových rizík DSA uvádza nasledovné povinnosti:

Článok	Opatrenie
Článok 26	Posúdenie rizika
Článok 27	Zmierňovanie rizík (opatrenia)
Článok 28	Nezávislé audity
Článok 29	Odporúčacie systémy
Článok 30	Dodatočná transparentnosť online reklamy
Článok 31	Prístup k údajom a ich kontrola
Článok 32	Pracovníci zodpovední za dodržiavanie súladu s predpismi
Článok 33	Povinnosti veľmi veľkých online platforiem podávať správy o transparentnosti

Najvypuklejšie požiadavky na bezpečnosť sú ustanovené v článku 31 DSA, ktorý upravuje prístup k údajom veľmi veľkých online platforiem a ich kontrolu. O tieto údaje môžu požiadať jednak dezignované orgány verejnej moci (koordinátori digitálnych služieb) a preverení výskumníci. Oba typy subjektov musia pri prístupe k údajom dodržiavať „osobitné požiadavky na bezpečnosť a dôvernosť údajov.“⁷⁷ Komisia zároveň môže prijať delegované akty, ktoré budú špecifikovať tieto mechanizmy aj z hľadiska rešpektovania práv tretích strán vrátane zachovávania bezpečnosti služieb digitálnych platforiem.⁷⁸

Zároveň, môžu veľmi veľké platformy podľa článku 33 (správy o transparentnosti) niektoré informácie nezverejňovať, ak by to ohrozilo bezpečnosť digitálnych služieb prípadne verejnú bezpečnosť.⁷⁹ Ide tak o poistku, aby nebolo nutné zverejňovať údaje, ktoré by napríklad mohli viesť ku efektívnejším kybernetickým útokom alebo „gamingu“ automatizovaných procesov.⁸⁰

Úloha pre MIRRI

Monitorovať prijímanie DSA a požiadaviek na digitálne služby z hľadiska kybernetickej bezpečnosti. Ak bude zriadený koordinátor digitálnych služieb podľa DSA, MIRRI môže novému subjektu poskytovať cenné know-how a odporúčania pri kontrole požiadaviek na kybernetickú bezpečnosť subjektov v pôsobnosti DSA.

⁷⁶ DSA, článok 26 ods. 1.

⁷⁷ DSA, článok 31 ods. 4.

⁷⁸ DSA, článok 31 ods. 5.

⁷⁹ DSA, článok 33 ods. 3.

⁸⁰ Pozri napríklad WANG, Q. et al. "Algorithmic transparency with strategic users." Available at SSRN 3652656 (2020).

2.2.4. Elektronická identifikácia

Problematika elektronickej identifikácie je na úrovni práva EÚ upravená v Nariadení eIDAS, ktorého cieľom je posilniť dôveru pri elektronických transakciách na vnútornom trhu. Tento cieľ sa má naplniť zabezpečením spoločného základu pre bezpečné elektronické interakcie medzi občanmi, podnikmi a orgánmi verejnej správy, čím sa zvýši účinnosť verejných a súkromných služieb online, elektronického podnikania a elektronického obchodu v EÚ.⁸¹

Prijatie Nariadenia eIDAS je výsledkom iniciatív viacerých európskych inštitúcií, ktoré dlhodobo upozorňovali na nedostatočné fungovanie jednotného digitálneho trhu, ktorý by mal uľahčiť cezhraničné používanie služieb online pričom osobitná pozornosť sa má venovať bezpečnej elektronickej identifikácii a autentifikácii.⁸²

2.2.4.1. Pôsobnosť

Vo všeobecnosti možno povedať, že Nariadenie eIDAS upravuje dve oblasti. Prvou oblasťou je problematika vzájomného uznávania prostriedkov elektronickej identifikácie. Ustanovenia týkajúce sa vzájomného uznávania prostriedkov elektronickej identifikácie majú zabezpečiť, aby fyzické osoby, právnické osoby a fyzické osoby zastupujúce právnické osoby mohli byť identifikované a autentifikované pri prístupe k online službám, ktoré poskytuje iný členský štát. Na tento účel sa nezavádza jeden prostriedok elektronickej identifikácie, ktorý by využívali všetci občania EÚ. Po splnení požiadaviek v zmysle Nariadenia eIDAS sa občania môžu identifikovať a autentifikovať do online služieb iných členských štátov aj prostredníctvom svojich národných prostriedkov elektronickej identifikácie.

Druhou oblasťou je problematika dôveryhodných služieb, ktoré sa týkajú vyhotovovania, overovania a validácie elektronických podpisov, elektronických pečatí alebo elektronických časových pečatí, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, certifikátov pre autentifikáciu webových sídiel, ako aj uchovávanie elektronických podpisov, pečatí alebo certifikátov, ktoré s týmito službami súvisia. Táto oblasť nadväzuje na inštitúty, ktoré už upravovala Smernica o EP, zavádzajú sa však aj nové elektronické nástroje, ako elektronická pečať, elektronické doručovacie služby či autentifikácia webových sídiel.⁸³

Rozsah pôsobnosti Nariadenia eIDAS je vymedzený pozitívne a negatívne. Nariadenie eIDAS sa vzťahuje len na schémy elektronickej identifikácie, ktoré boli oznámené členskými štátmi EÚ v zmysle Nariadenia eIDAS a na poskytovateľov dôveryhodných služieb, ktorí sú usadení v EÚ.⁸⁴

Nariadenie eIDAS sa nevzťahuje na poskytovanie dôveryhodných služieb, ktoré sa používajú výhradne v uzavretých systémoch na základe vnútroštátneho práva alebo dohôd medzi vymedzenou skupinou účastníkov. Takéto uzavreté systémy nemôžu mať vplyv na tretie strany. Ako príklad možno

⁸¹ Nariadenie eIDAS, recitál 2.

⁸² Nariadenie eIDAS, recitál 2.

⁸³ Nariadenie eIDAS, článok 1 písm. b) a c).

⁸⁴ Nariadenie eIDAS, článok 2 ods. 1.

uviesť systémy, ktoré zriadili podniky alebo orgány verejnej správy na riadenie vnútorných postupov a v rámci ktorých sa využívajú dôveryhodné služby.⁸⁵

2.2.4.2. Kybernetická bezpečnosť

Jedným z cieľov Nariadenia eIDAS je zabezpečiť, aby bola možná bezpečná elektronická identifikácia a autentifikácia⁸⁶ pri prístupe k cezhraničným službám online, ktoré ponúkajú členské štáty.⁸⁷

Kľúčom k dôveryhodnému cezhraničnému vzájomnému uznávaniu prostriedkov elektronickej identifikácie je **bezpečnosť** schém elektronickej identifikácie.⁸⁸

Narušenie bezpečnosti schémy elektronickej identifikácie je upravená v článku 10 Nariadenia eIDAS. Predmetné ustanovenie Nariadenia eIDAS upravuje situáciu, kedy oznámená schéma elektronickej identifikácie bola narušená alebo čiastočne skompromitovaná spôsobom, ktorý ovplyvní spoľahlivosť cezhraničnej autentifikácie danej schémy. V takýchto prípadoch je dotknutý členský štát povinný danú cezhraničnú autentifikáciu alebo dotknuté skompromitované časti bezodkladne pozastaviť alebo zrušiť a informuje o tom ostatné členské štáty a Komisiu.

V prípade ak dôjde k náprave narušenia alebo skompromitovania schémy elektronickej identifikácie, dotknutý členský štát cezhraničnú autentifikáciu opätovne zavedie a bez zbytočného odkladu o tom informuje ostatné členské štáty a Komisiu. V opačnom prípade, a teda ak sa narušenie alebo skompromitovanie neodstráni v lehote troch mesiacov od pozastavenia alebo zrušenia, dotknutý členský štát informuje ostatné členské štáty a Komisiu o stiahnutí schémy elektronickej identifikácie. Komisia bez zbytočného odkladu uverejní zodpovedajúce zmeny v zozname schém elektronickej identifikácie v Úradnom vestníku Európskej únie.⁸⁹

V podmienkach Slovenskej republiky možno hovoriť o narušení alebo skompromitovaní schémy elektronickej identifikácie v prípade, ak by bol narušený alebo skompromitovaný modul IAM (Identity Access Management), taktiež známy ako autentifikačný modul, ktorý plní dôležitú úlohu pri cezhraničnej autentifikácii osôb.

Bezpečná schéma elektronickej identifikácie, ktorá zabezpečuje spoľahlivú cezhraničnú autentifikáciu osôb do značnej miery súvisí a závisí od dostatočnej ochrany osobných údajov. V prvom rade, ak dôjde k úspešnej cezhraničnej autentifikácii sú osobám iných členských štátov zapísané osobné údaje do modulu IAM. Akékoľvek narušenie dôvernosti, integrity a dostupnosti údajov v procese cezhraničnej autentifikácie bude mať za následok porušenie ochrany osobných údajov.

⁸⁵ Nariadenia eIDAS, recitál 21.

⁸⁶ V zmysle bodu 7 preambuly vykonávacieho nariadenia Komisie (EÚ) 2015/1502 z 8. septembra 2015, ktorým sa stanovujú minimálne technické špecifikácie a postupy pre úrovne zabezpečenia prostriedkov elektronickej identifikácie podľa článku 8 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu by sa na zvýšenie bezpečnosti procesu autentifikácie mal používať väčší počet faktorov autentifikácie, a najmä z rôznych kategórií faktorov. Ako príklady sa uvádzajú spoločné tajomstvá, fyzické zariadenia a fyzické vlastnosti.

⁸⁷ Nariadenia eIDAS, recitál 12.

⁸⁸ Nariadenia eIDAS, recitál 19.

⁸⁹ Nariadenie eIDAS, čl. 10, ods. 2-3.

Aspekty kybernetickej bezpečnosti sú taktiež obsiahnuté v článku 19 Nariadenia eIDAS, ktoré upravuje špecifické bezpečnostné požiadavky uplatniteľné na poskytovateľov dôveryhodných služieb. Vzhľadom na to, že poskytovateľ dôveryhodných služieb má napríklad pri overovaní elektronických podpisov či pečatí nezastupiteľnú úlohu, zákonodarca kladie dôraz na ustanovenie presných bezpečnostných požiadaviek. Všeobecná požiadavka sa týka prijatia vhodných technických a organizačných opatrení na riadenie rizík ohrozujúcich bezpečnosť dôveryhodných služieb, ktoré poskytujú. Prijatím takýchto opatrení sa má zaistiť úroveň bezpečnosti primeraná stupňu rizika. Prijmú sa najmä opatrenia na prevenciu a minimalizáciu vplyvu bezpečnostných incidentov a na oznámenie nepriaznivých účinkov všetkých takýchto incidentov zainteresovaným stranám.⁹⁰

Poskytovatelia dôveryhodných služieb sú povinní oznamovať incidenty. Opätovne sa rozlišuje medzi nahlasovaním kompetentnému orgánu – v tomto prípade Národný bezpečnostný úrad SR a dotknutým osobám. Nariadenie eIDAS v článku 19 ods. 2 vyžaduje nahlásenie akéhokoľvek narušenia bezpečnosti alebo integrity s významným vplyvom na poskytovanú dôveryhodnú službu alebo osobné údaje uchovávané v rámci nej s lehotou bez zbytočného odkladu, najneskôr do 24 hodín. V prípade negatívneho vplyvu na dotknutú fyzickú, ale aj právnickú osobu sa incident nahlási aj priamo týmto osobám.

V prípade incidentu, ktorého narušenie bezpečnosti alebo integrity sa týka dvoch alebo viacerých členských štátov, národný orgán dohľadu, komu bol incident oznámený, informuje, ak je to vhodné, orgány dohľadu v ostatných dotknutých členských štátoch a agentúru ENISA. Taktiež platí, ak informovaný orgán dohľadu usúdi, že zverejnenie narušenia bezpečnosti alebo integrity je vo verejnom záujme, informuje o ňom verejnosť, alebo o to požiada poskytovateľa dôveryhodných služieb.⁹¹

K aprílu 2022 je v legislatívnom procese návrh na zmenu Nariadenia eIDAS, ktorý má okrem iného ambíciu zaviesť digitálnu identitu. Jedným z cieľov revízie Nariadenia eIDAS je zabezpečiť dôveru a bezpečnosť cezhraničného riešenia digitálnej identity.⁹²

Úloha pre MIRRI

Monitorovať prijímanie revízie Nariadenia eIDAS z hľadiska kybernetickej bezpečnosti.

2.2.5. Smernica NIS

Riadne fungovanie vnútorného trhu závisí od bezpečnosti sietí a informačných systémov, prostredníctvom ktorých sa poskytujú služby, ktoré majú zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností. Bezpečnosť sietí a informačných systémov je základným predpokladom hladkého fungovania vnútorného trhu.⁹³

⁹⁰ Nariadenie eIDAS, článok 19 ods. 1.

⁹¹ Nariadenie eIDAS, článok 19 ods. 2.

⁹² Bližšie pozri: <https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:52021PC0281&from=EN>.

⁹³ Smernica NIS, recitál 1 a 3.

V Smernici NIS sú definované dva druhy hospodárskych subjektov, a to konkrétne **prevádzkovatelia základných služieb** (ďalej aj ako „PZS“) a **poskytovatelia digitálnych služieb** (ďalej aj ako „PDS“). Popri týchto subjektoch sú adresátmi právnych noriem obsiahnutých v Smernici NIS aj samotné členské štáty, ktoré musia plniť konkrétne povinnosti.

Prevádzkovatelia základných služieb sú verejné alebo súkromné subjekty, ktoré spĺňajú kritéria v zmysle čl. 5 ods. 2 Smernice NIS a typ takéhoto subjektu sa uvádza v prílohe II Smernice NIS. Ide o subjekty z odvetvia:

- energetiky,
- dopravy,
- bankovníctva,
- infraštruktúry finančných trhov,
- zdravotníctva,
- dodávky a distribúcie pitnej vody a
- digitálnej infraštruktúry.

Smernica NIS umožňuje členským štátom regulovať PZS podľa **zásady minimálnej harmonizácie**, čo znamená, že je možné, aby si členské štáty túto úpravu rozšírili i na ďalšie, smernicou neuvedené odvetvia. Slovenská republika pridala odvetvie **verejná správa** či pošta. Niektoré členské štáty pridali odvetvia ako sociálne služby, vzdelávanie, životné prostredie či potraviny.

Smernica NIS v súvislosti s poskytovateľmi digitálnych služieb uplatňuje **princíp maximálnej harmonizácie**, čo znamená, že na rozdiel od úpravy PZS, nesmú členské štáty v prípade PDS prijať prísnejšie pravidlá, ako tie ktoré vyplývajú zo Smernice NIS. Poskytovatelia digitálnych služieb nepodliehajú procesu identifikácie ako v prípade PZS, nakoľko rozsah pôsobnosti Smernice NIS sa vzťahuje na všetkých PDS, ktorí napĺňajú definičné znaky pojmu PDS. Poskytovateľom digitálnych služieb je každá právnická osoba, ktorá poskytuje niektorú z týchto digitálnych služieb:

- a) online trhovisko,
- b) internetový vyhľadávač,
- c) služby cloud computingu,

2.2.5.1. Pôsobnosť

Právna úprava kybernetickej bezpečnosti v Smernici NIS nie je priamo orientovaná na ochranu fyzických a právnických osôb a nepriznáva im konkrétne práva v tejto oblasti. Smernica NIS stanovuje **opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov** v rámci EÚ s cieľom zlepšiť fungovanie vnútorného trhu. Na tento účel sa:

- *stanovujú pre všetky členské štáty povinnosti prijať **národnú stratégiu** v oblasti bezpečnosti sietí a informačných systémov,*

- vytvára **skupina pre spoluprácu** s cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi a rozvíjať vzájomnú dôveru medzi nimi,
- vytvára **sieť jednotiek pre riešenie počítačových bezpečnostných incidentov** (*computer security incident response teams network* – ďalej len „sieť jednotiek CSIRT“) s cieľom prispievať k rozvoju dôvery medzi členskými štátmi a podporovať rýchlu a účinnú operačnú spoluprácu,
- stanovujú **bezpečnostné a oznamovacie požiadavky** pre prevádzkovateľov základných služieb a pre poskytovateľov digitálnych služieb,
- stanovujú povinnosti členských štátov určiť **príslušné vnútroštátne orgány, národné jednotné kontaktné miesta a jednotky CSIRT** s úlohami súvisiacimi s bezpečnosťou sietí a informačných systémov

Smernica NIS je **všeobecným právnym predpisom** (*lex generalis*) v oblasti kybernetickej bezpečnosti. V prípade ak sa podľa právneho aktu EÚ špecifického (*lex specialis*) pre určité odvetvie vyžaduje, aby prevádzkovatelia základných služieb alebo poskytovatelia digitálnych služieb buď **zaistovali bezpečnosť** ich sietí a informačných systémov, alebo aby **oznamovali incidenty**, uplatňujú sa ustanovenia tohto právneho aktu EÚ špecifického pre určité odvetvie. Podmienkou pre uplatnenie špecifického právneho aktu EÚ je, aby tieto požiadavky mali **aspoň rovnocenný účinok** ako povinnosti stanovené v smernici NIS.⁹⁴

2.2.5.2. Kybernetická bezpečnosť

Napriek skutočnosti, že ide o legislatívny akt z oblasti kybernetickej bezpečnosti, Smernica NIS neupravuje pojem kybernetická bezpečnosť, ale definuje pojem **bezpečnosť sietí a informačných systémov**.

V zmysle čl. 4 ods. 1 Smernice NIS predstavuje bezpečnosť sietí a informačných systémov: „*schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, autentickosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.*“

V zmysle recitálu 3 Smernice NIS zohrávajú siete a informačné systémy, a predovšetkým Internet zásadnú úlohu pri uľahčovaní cezhraničného pohybu tovaru, služieb a osôb. Z dôvodu tohto nadnárodného charakteru môžu mať zásadné narušenia týchto systémov, či už úmyselné, alebo nie a bez ohľadu na to, kde k nim dôjde, dôsledky pre jednotlivé členské štáty aj EÚ ako celok. V tejto súvislosti je bezpečnosť sietí a informačných systémov základným predpokladom hladkého fungovania vnútorného trhu.

⁹⁴ Smernica NIS, článok 1 ods. 7.

Prevádzkovatelia základných služieb sú povinní **prijat' vhodné a primerané technické a organizačné opatrenia** na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke a taktiež sú povinní prijať primerané bezpečnostné 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.⁹⁵

Smernica NIS nedefinuje konkrétne druhy technických a organizačných opatrení. Je na členských štátoch, aké bezpečnostné požiadavky budú od konkrétnych subjektov vyžadovať, avšak tieto požiadavky musia dosiahnuť cieľ, ktorým je dostatočná úroveň bezpečnosti sietí a informačných systémov.

Ďalšie povinnosti sa týkajú **oznamovania incidentov**, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú. Smernica NIS definuje incident ako: „*každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov.*“ Prevádzkovatelia základných služieb nie sú povinní hlásiť všetky incidenty, ale len tie, ktoré majú **závažný vplyv na kontinuitu základných služieb**, ktoré poskytujú.⁹⁶ S cieľom určiť závažnosť vplyvu incidentu sa zohľadnia najmä tieto parametre:

- a) počet používateľov postihnutých narušením základnej služby;
- b) dĺžka trvania incidentu;
- c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol.⁹⁷

Smernica NIS nešpecifikuje **lehotu** na oznámenie incidentov, ale len ukladá povinnosť pre PZS, aby **bez zbytočného odkladu** oznamovali príslušnému orgánu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú.⁹⁸

Oznámenia o incidentoch, ktoré majú závažný vplyv na kontinuitu základných služieb obsahujú informácie umožňujúce príslušnému orgánu alebo jednotke CSIRT určiť prípadný **cezhraničný vplyv incidentu**. Na základe týchto informácií, ktoré poskytol PZS v oznámení, je príslušný orgán alebo jednotka CSIRT povinná informovať ostatné postihnuté členské štáty, ak má incident závažný vplyv na kontinuitu základných služieb v týchto členských štátoch.⁹⁹

Smernica NIS taktiež upravuje možnosť **informovania verejnosti o incidente**. Príslušný orgán alebo jednotka CSIRT môže informovať o jednotlivých incidentoch verejnosť za splnenia dvoch podmienok. **Prvou** podmienkou je, aby došlo k porade príslušného orgánu alebo jednotky CSIRT s oznamujúcim PZS. Z tejto podmienky vyplýva, že príslušný orgán alebo jednotka CSIRT nemôže informovať o incidente verejnosť, pokiaľ to nebude prekonzultované s PZS, ktorého sa incident týka. **Druhá** kumulatívna podmienka je, aby bola informovanosť verejnosti potrebná na zabránenie incidentu alebo na riešenie prebiehajúceho incidentu.¹⁰⁰

⁹⁵ Smernica NIS, článok 14 ods. 1 a 2.

⁹⁶ Smernica NIS, článok 14 ods. 3.

⁹⁷ Smernica NIS, článok 14 ods. 3.

⁹⁸ Smernica NIS, článok 14 ods. 3.

⁹⁹ Smernica NIS, článok 14 ods. 3 a ods. 5.

¹⁰⁰ Smernica NIS, článok 14 ods. 6.

Popri povinnom hlásení kybernetických bezpečnostných incidentoch upravuje Smernica NIS aj **dobrovoľné oznamovanie**. Subjekty, ktoré neboli určené ako PZS a nie sú PDS, môžu na dobrovoľnom základe oznamovať incidenty, ktoré majú závažný vplyv na kontinuitu služieb, ktoré poskytujú.¹⁰¹

Poskytovatelia digitálnych služieb sú povinní plniť obdobné povinnosti ako PZS. Pre účely špecifikácie prvkov, ktoré musia PDS zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov a parametrov na posudzovanie toho, či má incident závažný vplyv bolo prijaté vykonávacie nariadenie Komisie (EÚ) 2018/151.

2.2.6. Akt o kybernetickej bezpečnosti

Ďalším legislatívnym aktom z oblasti kybernetickej bezpečnosti prijatým na úrovni EÚ je **Akt o kybernetickej bezpečnosti**. V recitáloch predmetného legislatívneho aktu sa podobne ako v prípade Smernice NIS vyzdvihuje dôležitosť sietí a informačných, ktoré sú schopné podporovať všetky aspekty nášho života a poháňať hospodársky rast EÚ. Tieto siete a informačné systémy sú považované za základné kamene pre dosiahnutie jednotného digitálneho trhu. Akt o kybernetickej bezpečnosti taktiež používa pojem informačné a komunikačné technológie (IKT), na ktorých sú založené komplexné systémy, ktoré podporujú každodenné činnosti spoločnosti, udržujú chod kľúčových odvetví hospodárstva, ako je zdravotníctvo, energetika, financie či doprava, a najmä podporujú fungovanie vnútorného trhu.¹⁰²

Ako sa uvádza v recitáli Aktu o kybernetickej bezpečnosti, incidenty oslabujú dôveru v poskytovateľov digitálnych služieb a v samotný jednotný digitálny trh, najmä medzi spotrebiteľmi. Posilnenie dôvery by mala môcť uľahčiť celožitná certifikácia, ktorou sa zabezpečia spoločné požiadavky kybernetickej bezpečnosti na produkty IKT, služby IKT a procesy IKT a hodnotiace kritériá naprieč vnútroštátnymi trhmi a odvetviami.¹⁰³

2.2.6.1. Pôsobnosť

Akt o kybernetickej bezpečnosti si podobne ako Smernica NIS kladie za cieľ zaistiť riadne fungovanie vnútorného trhu, avšak navyše sa usiluje o dosiahnutie vysokej úrovne kybernetickej bezpečnosti, kybernetickej odolnosti a dôvery v rámci EÚ. Na splnenie týchto cieľov sa:

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

¹⁰¹ Smernica NIS, článok 20 ods. 1.

¹⁰² Akt o kybernetickej bezpečnosti, recitál 1 a 2.

¹⁰³ Akt o kybernetickej bezpečnosti, recitál 7.

- vytvára rámec pre zavádzanie **európskych systémov certifikácie kybernetickej bezpečnosti** na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v EÚ.¹⁰⁴

Agentúra ENISA je právnou nástupkyňou Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť a sídli v Grécku. Plnením úloh, ktoré agentúre ENISA boli zverené aktom o kybernetickej bezpečnosti, sa má dosiahnuť vysoká spoločná úroveň kybernetickej bezpečnosti v celej EÚ a prispieť k zníženiu fragmentácie vnútorného trhu.¹⁰⁵

Medzi úlohy Agentúry ENISA patrí napr. pomoc pri tvorbe legislatívnych iniciatív, ktoré sa týkajú kybernetickej bezpečnosti, najmä poskytovaním nezávislých stanovísk a analýz. Taktiež pomáha členským štátom pri konzistentnom vykonávaní politiky a práva EÚ v oblasti kybernetickej bezpečnosti, najmä v súvislosti so Smernicou NIS, a to aj vydávaním stanovísk, usmernení, poskytovaním poradenstva a pod.¹⁰⁶

Agentúra ENISA pomáha členským štátom v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických hrozieb a incidentov a schopnosť reagovať na ne tým, že im poskytuje vedomosti a odborné znalosti. Taktiež pravidelne organizuje kybernetickobezpečnostné cvičenia na úrovni EÚ a analyzuje nastupujúce technológie a poskytuje tematicky zamerané posúdenia očakávaných spoločenských, právnych, hospodárskych a regulačných vplyvov technologických inovácií na kybernetickú bezpečnosť.¹⁰⁷

2.2.6.2. Kybernetická bezpečnosť

Akt o kybernetickej bezpečnosti obsahuje **prvú legálnu definíciu pojmu kybernetická bezpečnosť** na úrovni práva EÚ, v zmysle ktorej je kybernetická bezpečnosť definovaná ako: **„činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami.“**¹⁰⁸

Pri porovnaní pojmu kybernetická bezpečnosť a pojmu bezpečnosť sietí a informačných systémov v zmysle Smernice NIS, možno vidieť niekoľko odlišností. Zatiaľ, čo pri pojme bezpečnosť sietí a informačných je hlavným cieľom odolávať konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernoscť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb, v prípade pojmu kybernetická bezpečnosť je cieľom ochrana sietí a informačných systémov, užívateľov takýchto systémov a iných osôb. Taktiež v prípade definície pojmu kybernetická bezpečnosť možno vidieť, že je potrebné chrániť nielen siete a informačné systémy, ale aj ich **užívateľov a iné osoby, dotknuté kybernetickými hrozbami**. V porovnaní s definíciou bezpečnosti sietí a informačných systémov použitej v Smernici NIS ide o výrazný posun, čo do **ochrany fyzických a právnických**

¹⁰⁴ Akt o kybernetickej bezpečnosti, článok 1 ods. 1.

¹⁰⁵ Akt o kybernetickej bezpečnosti, článok 3 ods. 1.

¹⁰⁶ Akt o kybernetickej bezpečnosti, článok 5 ods. 2.

¹⁰⁷ Akt o kybernetickej bezpečnosti, článok 6, 7, 9.

¹⁰⁸ Akt o kybernetickej bezpečnosti, článok 2 bod 1.

osôb pred kybernetickými hrozbami. Vyššie uvedené potvrdzuje aj recitál 3 Aktu o kybernetickej bezpečnosti.

V recitáli 3 Aktu o kybernetickej bezpečnosti je vyjadrená potreba ochrany fyzických osôb nasledovne: *„Rastúca digitalizácia a pripojiteľnosť zvyšujú kybernetickobezpečnostné riziká, takže spoločnosť ako celok sa stáva zraniteľnejšou z hľadiska kybernetických hrozieb a zvyšuje sa nebezpečenstvo, ktorému čelia fyzické osoby, vrátane zraniteľných osôb, ako sú napríklad deti.“*

Kybernetické hrozby môžu mať negatívny vplyv aj na samotné deti. V súčasnosti možno medzi najčastejšie sa vyskytujúce hrozby pre deti v online prostredí zaradiť kyberšikanu, nevhodný obsah (intímne alebo sexuálne explicitné obrázky či videá), sexting (posielanie sexuálne explicitných správ a intímnych fotiek), sextortion (útočník požaduje výkupné v opačnom prípade zverejní intímne fotografie obete), nadmerné zdieľanie osobných údajov či online predátorstvo.

Posun k ochrane fyzických osôb je potvrdený aj v recitáli 8, v zmysle ktorého kybernetická bezpečnosť nie je len otázkou technológie, ale rovnako dôležité je aj správanie ľudí. Mala by sa preto významne podporovať tzv. **kybernetická hygiena**, konkrétne jednoduché rutinné opatrenia, ktoré minimalizujú vystavenie sa rizikám kybernetických hrozieb, ak ich občania, organizácie a podniky vykonávajú pravidelne.¹⁰⁹

Akt o kybernetickej bezpečnosti definuje pojem **kybernetická hrozba** ako: *„každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť sieť a informačné systémy, užívateľov takýchto systémov a iné osoby.“*¹¹⁰ Z vyššie uvedenej definície vyplýva, že nielen sieť a informačné systémy, ale aj užívatelia takýchto systémov a iné osoby môžu byť poškodené, narušené alebo inak negatívne ovplyvnené. Predmetná definícia sa teda týka všetkých osôb, nie len samotných užívateľov konkrétnych systémov.

Akt o kybernetickej bezpečnosti vytvára **systém certifikácie v oblasti kybernetickej bezpečnosti**, ktorý by mal zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti produktov, postupov a služieb v EÚ. Je potrebné podotknúť, že akt o kybernetickej bezpečnosti nevytvára jednotlivé certifikačné schémy ale vytvára rámec pre prijímanie európskych certifikačných schém.

Certifikácia IKT v oblasti kybernetickej bezpečnosti sa stáva veľmi dôležitou otázkou, a to najmä vo vzťahu k zvýšenému používaniu technológií, ktoré požadujú vysokú úroveň kybernetickej bezpečnosti. Predmetné nariadenie ako príklady technológií, pri ktorých je potrebné zabezpečiť vysokú úroveň kybernetickej bezpečnosti uvádza autonómne vozidlá, systémy elektronickej kontroly zdravia alebo priemyselnej automatizácie.

V zmysle Aktu o kybernetickej bezpečnosti možno certifikovať produkty IKT (napr. router), služby IKT (napr. autentifikácia klientov online) a procesy IKT (napr. systém riadenia bezpečnosti informácií).

¹⁰⁹ Akt o kybernetickej bezpečnosti, recitál 8.

¹¹⁰ Akt o kybernetickej bezpečnosti, článok 2 bod 8.

2.2.7. Návrh smernice NIS 2

Európska komisia koncom decembra 2020 predstavila balík opatrení a právnych aktov v oblasti kybernetickej bezpečnosti s cieľom modernizácie tohto právneho rámca. Na úrovni EÚ boli konkrétne predstavené Stratégia kybernetickej bezpečnosti EÚ pre digitálnu dekádu,¹¹¹ Návrh smernice o odolnosti kritických subjektov a **Návrh smernice NIS 2**.

Pravidelný prieskum Smernice NIS ukázal viaceré nedostatky súčasnej právnej úpravy. Predmetný prieskum bol zároveň aj základom pre vypracovanie znenia Návrhu smernice NIS 2.¹¹²

Európska komisia z dôvodu modernizácie právneho rámca v dôsledku dynamickej digitalizácie verejných a súkromných služieb, ako aj zvýšeniu ich využívania počas prebiehajúcej pandémie COVID-19 pristúpila k revízií Smernice NIS. Ako hlavné dôvody revízie sa v dôvodovej správe k Návrhu smernice NIS 2 uvádzajú:

- nízka úroveň kybernetickej odolnosti podnikov pôsobiach v EÚ;
- nejednotná úroveň odolnosti v jednotlivých členských štátoch a odvetviach; a
- nízka úroveň spoločnej situačnej informovanosti a nedostatočná spoločná reakcia na krízu.

Ako jasný príklad nejednotnosti Európska komisia spomína prípad poskytovateľov zdravotnej starostlivosti, ktoré v niektorých členských štátoch EÚ patria do rozsahu implementácie Smernice NIS a podliehajú bezpečnostným a organizačným požiadavkám na kybernetickú bezpečnosť a naopak, v niektorých členských štátoch týmto požiadavkám musia prispôsobiť procesy iba väčšie nemocnice.

Od prijatia nového právneho rámca v oblasti kybernetickej bezpečnosti si Európska komisia sľubuje predovšetkým dosiahnuť **troch klúčových cieľov**. Prvým je zvýšenie úrovne kybernetickej bezpečnosti naprieč všetkými relevantnými sektormi, čo v konečnom dôsledku prinesie vyššie benefity pre ekonomiku a spoločnosť ako celok. Druhým cieľom je zníženie nezrovnalostí na vnútornom trhu EÚ v sektoroch, ktoré už v súčasnosti pokrýva Smernica NIS. Tretím cieľom je zlepšenie úrovne spoločného povedomia a kolektívnej schopnosti pripraviť sa a reagovať na kybernetické hrozby v jednotlivých členských štátoch z pohľadu orgánov verejnej moci.¹¹³

2.2.7.1. Pôsobnosť

Návrh smernice NIS 2 neukladá členským štátom povinnosť identifikovať subjekty, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb („proces identifikácie“), tak ako to je upravené v Smernici NIS. Namiesto toho sa v Návrhu smernice NIS 2 stanovilo **jednotné kritérium**, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice.

¹¹¹ Dostupné na: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.

¹¹² Z daného posúdenia vyplýva 6 oblastí, ktoré ukázali najvyššiu mieru nedostatočnosti. Konkrétne: Nedostatočná prepojenosť požiadaviek Smernice NIS pre jednotlivé sektory; Nejasné vymedzenie pôsobnosti smernice a nejasné vymedzenie kompetencií národných dozorných autorít; Odlišné bezpečnostné a notifikačné povinnosti naprieč členskými štátmi; Nedostatočne efektívny dohľad a vymáhanie; Neporovnateľné prerozdelenie financií pri otázkach kybernetickej bezpečnosti naprieč členskými štátmi; Limitované zdieľanie informácií medzi členskými štátmi.

¹¹³ Tamže, s. 31.

Toto kritérium spočíva v uplatňovaní **pravidla obmedzenia veľkosti** (*size-cap rule*), podľa ktorého sa Návrh smernice NIS 2 nevzťahuje na subjekty, ktoré v zmysle **Odporúčanie Komisie 2003/361/ES** spĺňajú kritériá mikropodniku¹¹⁴ alebo malého podniku.¹¹⁵

Z iného uhla pohľadu si pravidlo obmedzenia veľkosti možno vykladať aj spôsobom, že do rozsahu pôsobnosti Návrhu smernice NIS 2 patria všetky stredné¹¹⁶ a veľké podniky, ako sú vymedzené v Odporúčaní Komisie 2003/361/ES, ktoré pôsobia v rámci odvetví uvedených v prílohe I alebo prílohe II Návrhu smernice NIS 2.

Od členských štátov sa nevyžaduje, aby zostavili zoznam subjektov, ktoré spĺňajú toto všeobecne uplatniteľné kritérium týkajúce sa veľkosti.

Výnimka z pravidla obmedzenia veľkosti

Zo všeobecného pravidla obmedzenia veľkosti existuje v zmysle Návrhu smernice NIS 2 aj výnimka. Výnimku z pravidla obmedzenia veľkosti predstavujú tie mikropodniky alebo makropodniky uvedené v prílohe I a II, ktoré spĺňajúce určité kritériá, ktoré sú ukazovateľom kľúčovej úlohy pre hospodárstva alebo spoločnosti členských štátov alebo pre určité odvetvia či druhy služieb.

Konkrétne sa Návrh smernice NIS 2 vzťahuje aj na subjekty, ktorého typ je uvedený v prílohe I alebo prílohe II bez ohľadu na ich veľkosť keď:¹¹⁷

- a) *služby poskytuje jeden z týchto subjektov:*
 - i. *verejné elektronické komunikačné siete alebo verejne dostupné elektronické komunikačné služby uvedené v bode 8 prílohy I;*
 - ii. *poskytovatelia dôveryhodných služieb uvedení v bode 8 prílohy I;*
 - iii. *správcovia mien domény najvyššej úrovne a poskytovatelia služby systému doménových mien (DNS) uvedení v bode 8 prílohy I;*
- b) *subjekt je subjektom verejnej správy podľa vymedzenia v článku 4 bode 23;*
- c) *subjekt je jediným poskytovateľom služby v členskom štáte;*
- d) *potenciálne narušenie služby poskytovanej subjektom by mohlo mať vplyv na ochranu verejnosti, verejnú bezpečnosť alebo verejné zdravie;*
- e) *potenciálne narušenie služby poskytovanej subjektom by mohlo vyvolať systémové riziká, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;*
- f) *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;*

¹¹⁴ Mikropodniky sa definujú ako podniky, ktoré zamestnávajú menej ako 10 osôb a ktorých ročný obrat alebo ročná bilančná suma nepresahuje 2 milióny eur.

¹¹⁵ Malé podniky sa definujú ako podniky, ktoré zamestnávajú menej ako 50 osôb a ktorých ročný obrat alebo ročná bilančná suma nepresahuje 10 miliónov eur.

¹¹⁶ Stredné podniky sú 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. Odporúčania Komisie 2003/361/ES.

¹¹⁷ Návrh smernice NIS 2, článok 2 ods. 2.

g) *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.*

Členské štáty vypracujú **zoznam** subjektov identifikovaných podľa písmen b) až f) a predložia ho Európskej komisii do 6 mesiacov po uplynutí lehoty na transpozíciu. Členské štáty zoznam pravidelne preskúmajú, a to následne aspoň každé dva roky a v prípade potreby ho aktualizujú.¹¹⁸

Návrh smernice NIS 2 ponecháva členským štátom pri tvorbe zoznamu tzv. dodatočných subjektov široký priestor na voľné konanie, čo môže podobne ako pri identifikácii prevádzkovateľov základných služieb podľa Smernice NIS viesť k právnej fragmentácii a nezabezpečí sa harmonizácia.

Subjekty verejnej správy ako kľúčové subjekty

Pre verejnú správu je najvýznamnejšou zmenou v prípade kľúčových subjektov pridanie sektora **Verejná správa** do prílohy I. V sektore Verejná správa sú uvedené konkrétne typy subjektov.

Návrh smernice NIS 2 taktiež zavádza pojem „**subjekt verejnej správy**“, ktorý má 4 definičné znaky. Správna interpretácia tohto pojmu bude veľmi dôležitá v prípade identifikácie subjektov verejnej správy, ktoré sú uvedené ako typ subjektu v sektore Verejná správa a spĺňajú definičné znaky tohto pojmu v zmysle Návrhu smernice NIS 2 pri uplatnení výnimky z pravidla obmedzenia veľkosti.

V rámci sektora Verejná správa sú uvedené 3 typy subjektov verejnej správy, konkrétne subjekty verejnej správy na úrovni ústrednej štátnej správy, Subjekty verejnej správy v regiónoch úrovne NUTS 1 a NUTS 2.¹¹⁹

Ako príklady subjektov verejnej správy možno uviesť správne orgány štátu (*administrative departments of the state*) a ďalšie ústredné orgány (*central agencies*), ktorých pôsobnosť pokrýva celé ekonomické územie krajiny (*whose responsibilities cover the whole economic territory of a country*).¹²⁰ V podmienkach Slovenskej republiky možno za subjekty verejnej správy na úrovni ústrednej štátnej správy považovať:

- ministerstvá a
- ostatné ústredné orgány štátnej správy.¹²¹

Za **subjekty verejnej správy v regiónoch úrovne NUTS 1 a NUTS 2** by sme mohli v podmienkach Slovenskej republiky považovať vyššie územné celky, ktoré predstavujú územné samosprávne a správne celky Slovenskej republiky a v jednotlivých regiónoch podľa úrovni NUTS 1 a

¹¹⁸ Návrh smernice NIS 2, článok 2 ods. 2.

¹¹⁹ Klasifikácia NUTS rozčleňuje v zmysle nariadenia (ES) č. 1059/2003 hospodárske územie členských štátov na územné jednotky troch úrovní (NUTS 1, NUTS 2 a NUTS 3). Táto klasifikácia je doplnená o lokálne administratívne jednotky (LAU), ktoré predstavujú podrobnejšie členenie úrovne NUTS 3.

¹²⁰ COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. Dostupné na: <https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A52020SC0345>, s. 51.

¹²¹ Bližšie pozri zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy.

NUTS 2 pre Slovenskú republiku, sú oprávnené prijímať administratívne alebo politické rozhodnutia pre danú oblasť v právnom a inštitucionálnom rámci Slovenskej republiky.¹²²

Úloha pre MIRRI

Monitorovať transpozíciu prijatého Návrhu smernice NIS 2, a to najmä s ohľadom na správnu interpretáciu pojmu subjekt verejnej správy v rámci nového sektora Verejná správa.

2.2.7.2. Kybernetická bezpečnosť

Návrh smernice NIS 2 pozmeňuje definície pojmov incident, závažný incident a používa pojmy prevzaté z Aktu o kybernetickej bezpečnosti ako kybernetická bezpečnosť či kybernetická hrozba. V návrhu sú taktiež nové definície pojmov ako zraniteľnosť, dátové centrum, sieť na sprístupňovanie obsahu či platforma služieb sociálnej siete.

Kľúčové a dôležité subjekty sú povinné bez zbytočného odkladu oznámiť príslušným orgánom alebo jednotke CSIRT každý incident so závažným vplyvom na poskytovanie ich služieb.¹²³

V Návrhu smernice NIS 2 je incident definovaný ako: *„každá udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.“*¹²⁴

Z vyššie uvedenej definície vyplýva, že za incident sa považuje udalosť, ktorá ohrozuje tri základné bezpečnostné požiadavky na ochranu informácií, ktorými sú dostupnosť, integrita a dôvernosť, ku ktorým sa pridáva aj pravosť. V zmysle tejto definície ohrozeniu podliehajú nie len údaje, ale aj súvisiace služby, ktoré sú poskytované alebo prístupné prostredníctvom sietí a informačných systémov.

Incident sa považuje za závažný, ak:¹²⁵

- a) dotknutému subjektu spôsobil alebo môže spôsobiť podstatné narušenie prevádzky alebo finančné straty;
- b) zasiahol alebo môže zasiahnuť iné fyzické alebo právnické osoby spôsobením značných hmotných alebo nehmotných strát.

Kľúčové a dôležité subjekty sú povinné na účely oznámenia závažných incidentov predložiť príslušným orgánom alebo jednotke CSIRT:¹²⁶

¹²² Pre účely stanovenia príslušnej úrovne NUTS, do ktorej sa má zaradiť určitá trieda administratívnych jednotiek v členskom štáte, sa zaviedli nasledujúce populačné prahy: NUTS 1 (minimum: 3 milióny; maximum 7 miliónov). NUTS 2 (minimum: 800 000; maximum 3 milióny). NUTS 3 (minimum: 150 000, maximum: 800 000). V prípade Slovenskej republiky ide konkrétne o nasledujúce úrovne NUTS: NUTS I – Slovensko. NUTS II - Bratislavský kraj, západné Slovensko, stredné Slovensko, východné Slovensko. NUTS III - Bratislavský kraj, Trnavský kraj, Trenčiansky kraj, Nitriansky kraj, Žilinský kraj, Banskobystrický kraj, Prešovský kraj, Košický kraj.

¹²³ Návrh smernice NIS 2, článok 20 ods. 1.

¹²⁴ Návrh smernice NIS 2, článok 4 bod 5.

¹²⁵ Návrh smernice NIS 2, článok 20 ods. 3.

¹²⁶ Návrh smernice NIS 2, článok 20 ods. 4.

- a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia incidentu prvotné oznámenie, v ktorom sa prípadne uvedie, či incident pravdepodobne spôsobilo nezákonné alebo zlomyseľné konanie;
- b) na žiadosť príslušného orgánu alebo jednotky CSIRT priebežnú správu o relevantných aktualizáciách daného stavu;
- c) najneskôr jeden mesiac po predložení prvotného oznámenia konečnú správu, ktorá obsahuje aspoň tieto informácie:
 - i. podrobný opis incidentu, jeho závažnosť a vplyv;
 - ii. druh hrozby alebo základnú príčinu, ktorá pravdepodobne incident spôsobila;
 - iii. uplatnené a prebiehajúce zmierňujúce opatrenia.

V riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkou CSIRT sa môžu kľúčové a dôležité subjekty odchýliť od lehôt stanovených v písmenách a) a c).¹²⁷

V prípade potreby kľúčové a dôležité subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb incidenty, ktoré by mohli nepriaznivo ovplyvniť ich poskytovanie.¹²⁸

Kľúčové a dôležité subjekty sú taktiež povinné oznamovať okrem iného informácie umožňujúce príslušným orgánom alebo jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu.¹²⁹

Kľúčové a dôležité subjekty sú okrem hlásenia incidentov so závažným vplyvom taktiež povinné bez zbytočného odkladu oznámiť príslušným orgánom alebo jednotke CSIRT každú závažnú kybernetickú hrozbu, ktorú kľúčové a dôležité subjekty zistia a ktorá by mohla potenciálne viesť k závažnému incidentu. Kybernetická hrozba predstavuje pojem, ktorý nie je definovaný v smernici NIS.¹³⁰

V príslušných prípadoch bez zbytočného odkladu oznámia kľúčové a dôležité subjekty príjemcom svojich služieb, ktorých potenciálne zasiahla závažná kybernetická hrozba, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať.¹³¹

Kľúčové a dôležité subjekty v prípade potreby týmto príjemcom oznámia aj informáciu o samotnej hrozbe. Oznámenie nesmie mať pre oznamujúci subjekt za následok vyššiu zodpovednosť.¹³²

2.2.7.3. Bezpečnostné opatrenia

Kľúčové a dôležité subjekty sú povinné prijať vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú pri poskytovaní svojich služieb. S ohľadom na najnovší technický vývoj (*state of the*

¹²⁷ Návrh smernice NIS 2, článok 20 ods. 4.

¹²⁸ Návrh smernice NIS 2, článok 20 ods. 1.

¹²⁹ Návrh smernice NIS 2, článok 20 ods. 1.

¹³⁰ Návrh smernice NIS 2, článok 20 ods. 2.

¹³¹ Návrh smernice NIS 2, článok 20 ods. 2.

¹³² Návrh smernice NIS 2, článok 20 ods. 2.

arť) tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika.¹³³

Návrh smernice NIS 2 definuje konkrétne druhy opatrení na riadenie kybernetickobezpečnostných rizík, ktoré majú kľúčové a dôležité subjekty prijať. Tieto opatrenia obsahujú aspoň:¹³⁴

- 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.

Pri zvažovaní vhodných opatrení uvedených v písmene d) sa musia zohľadňovať zraniteľnosti špecifické pre každého dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a prax ich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja.¹³⁵

V prípade ak subjekt zistí, že jeho služby alebo úlohy nie sú v súlade s opatreniami, je povinný prijať bez zbytočného odkladu všetky potrebné nápravné opatrenia a danú službu s týmito opatreniami zosúladiť.¹³⁶

S cieľom stanoviť technické a metodické špecifikácie opatrení môže Európska komisia prijať vykonávacie akty.¹³⁷

Výpočet vyššie uvedených opatrení nie je taxatívny. Európska komisia je oprávnená na prijímanie delegovaných aktov s cieľom doplniť opatrenia na zohľadnenie nových kybernetických hrozieb, technologického vývoja alebo odvetvových špecifik.¹³⁸

Úloha pre MIRRI

Monitorovať transpozíciu prijatého Návrhu smernice NIS 2 a to najmä s ohľadom na bezpečnostné opatrenia, ktoré budú musieť plniť subjekty verejnej správy v rámci nového sektora Verejná správa.

¹³³ Návrh smernice NIS 2, recitál 14 a čl. 18 ods. 1.

¹³⁴ Návrh smernice NIS 2, článok 18 ods. 2.

¹³⁵ Návrh smernice NIS 2, článok 18 ods. 3.

¹³⁶ Návrh smernice NIS 2, článok 18 ods. 4.

¹³⁷ Návrh smernice NIS 2, článok 18 ods. 5.

¹³⁸ Návrh smernice NIS 2, článok 18 ods. 6.

Zásadné zmeny sa týkajú aj otázok **dohľadu a presadzovania práva**. Návrh smernice NIS 2 v porovnaní so Smernicou NIS posilňuje právomoci a opatrenia v oblasti dohľadu a presadzovania práva. Pre tieto účely sa stanovil minimálny zoznam opatrení a prostriedkov dohľadu, prostredníctvom ktorých môžu príslušné orgány vykonávať dohľad nad kľúčovými a dôležitými subjektmi a taktiež minimálny zoznam správnych sankcií za porušenie povinností v oblasti riadenia kybernetickobezpečnostných rizík a oznamovania.

Zásadná zmena sa týka aj ukladania **správnych pokút**, ktoré možno uložiť do výšky 10 000 000 EUR alebo najviac 2 % celkového svetového ročného obratu podniku, ku ktorému kľúčový alebo dôležitý subjekt patrí, v predchádzajúcom účtovnom období, podľa toho, ktorá suma je vyššia.

Návrh smernice NIS 2 prináša nové požiadavky na vypracovanie **národných stratégií kybernetickej bezpečnosti**, ktoré musia byť komplexnejšie a adresnejšie ako doteraz. Prehlbujú sa požiadavky na úrovni vnútroštátnej spolupráci, ale hlavne na poli spolupráci medzinárodnej v rámci EÚ. Pomerne zásadná časť Návrhu smernice NIS 2 je venovaná zdieľaniu a výmene informácií, nie len medzi príslušnými subjektmi a jednotkami CSIRT, ale aj v rámci kľúčových a dôležitých subjektov.

Nové požiadavky sa týkajú **uchovávaní a prístupu k údajom** od správcov domén najvyššej úrovne a subjektom, ktorý ponúkajú registráciu domén ako službu. Viaceré ustanovenia reagujú na aj na potreby GDPR pri jasnom vymedzení kompetencií dozorných orgánov, právnych základov pre rôzne spracovateľské operácie či ukladanie sankcií. Zriadujú sa inštitúty partnerského preskúmania, koordinovaného zverejňovanie informácií o zraniteľnosti či európsky register zraniteľností.

2.2.8. Návrh smernice o odolnosti kritických subjektov

EÚ okrem revízie právneho rámca kybernetickej bezpečnosti v podobe Návrhu smernice NIS 2 predstavila **aj revíziu právnej úpravy kritickej infraštruktúry – Návrh smernice o odolnosti kritických subjektov**. Tento právny akt nahradí doteraz platnú Smernicu o európskej kritickej infraštruktúre.

Návrh smernice o odolnosti kritických subjektov sa výrazne prekrýva s Návrhom smernice NIS 2, ktorého cieľom je zvýšiť odolnosť informačných a komunikačných technológií kľúčových subjektov a dôležitých subjektov. Túto skutočnosť je vyjadrená aj v dôvodovej správe k Návrhu smernice o odolnosti kritických subjektov, v zmysle ktorej je Návrh smernice o odolnosti kritických subjektov predovšetkým v úzkom súlade a vytvára úzke synergie s Návrhom smernice NIS 2.¹³⁹

¹³⁹ Dôvodová správa, s. 4.

2.2.8.1. Pôsobnosť

Návrh smernice o odolnosti kritických subjektov **stanovuje**:

- a) **pre členské štáty povinnosť prijať určité opatrenia** zamerané na zabezpečenie poskytovania základných služieb, najmä identifikovať kritické subjekty a subjekty, s ktorými sa má v určitých ohľadoch zaobchádzať ako s rovnocennými, a umožniť im plniť si povinnosti;
- b) **pre kritické subjekty povinnosti** zamerané na **zvýšenie ich odolnosti** a zlepšenie ich schopnosti poskytovať tieto služby na vnútornom trhu;
- c) **vo vzťahu ku kritickým subjektom pravidlá dohľadu** a ich **presadzovania** a osobitný dohľad nad kritickými subjektmi, ktoré sa považujú za subjekty osobitného európskeho významu.

Návrh smernice o odolnosti kritických prvkov sa nevzťahuje na záležitosti, na ktoré sa vzťahuje Návrh smernice NIS 2. Avšak na subjekty identifikované ako kritické subjekty podľa Návrhu smernice o odolnosti kritických subjektov sa vzťahuje Návrh smernice NIS 2.¹⁴⁰

Návrh smernice o odolnosti kritických prvkov taktiež obsahuje ustanovenia, ktoré upravujú vzťah *lex specialis* k legislatívnym aktom EÚ, ktoré vyžadujú od kritických subjektov prijatie rovnakých opatrení. V prípade ak sa v ustanoveniach odvetvových aktov práva EÚ vyžaduje, aby kritické subjekty prijali opatrenia stanovené v kapitole III Návrhu smernice o odolnosti kritických subjektov, príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní uvedených sa neuplatňujú za podmienky, že tieto **požiadavky sú aspoň rovnocenné s povinnosťami stanovenými v tejto smernici**. Predmetné ustanovenie má za cieľ odstrániť duplicitu plnenia rovnakých opatrení kritickými subjektmi.

Zatiaľ čo sa Smernica o európskej kritickej infraštruktúre vzťahuje len na odvetvia energetiky a dopravy, Návrh smernice o odolnosti kritickej infraštruktúry rozširuje rozsah pôsobnosti aj na iné odvetvia. Konkrétne ide o nasledujúce odvetvia, ktoré sú uvedené v prílohe Návrhu smernice o odolnosti kritických prvkov:

1. energetika,
2. doprava,
3. bankovníctvo,
4. infraštruktúra finančného trhu,
5. zdravotníctvo,
6. pitná voda,
7. odpadová voda,
8. digitálna infraštruktúra,
9. verejná správa a

¹⁴⁰ Návrh smernice NIS 2, článok 2 ods. 2 písm. g).

10. vesmír.

Odvetvia uvedené v Návrhu smernice o odolnosti kritických subjektov kopírujú odvetvia upravené v Návrhu smernice NIS 2. V rámci niektorých odvetví boli zadefinované aj pododvetvia. V prílohe Návrhu smernice o odolnosti kritických subjektov sa nachádzajú aj typy subjektov v rámci konkrétneho odvetvia, resp. pododvetvia.

Z pohľadu zamerania a pôsobnosti **MIRRI** predstavuje významnú zmenu pridanie odvetvia **Verejná správa**, v rámci ktorého sú uvedené konkrétne **typy kritických subjektov**, konkrétne subjekty verejnej správy na úrovni ústrednej štátnej správy, subjekty verejnej správy v regiónoch úrovne NUTS 1 a NUTS 2.¹⁴¹

Členské štáty sú do troch rokov a troch mesiacov od nadobudnutia účinnosti smernice **povinné identifikovať kritické subjekty** pre každé odvetvie a pododvetvie uvedené v prílohe. Povinnosť identifikácie kritických subjektov sa netýka sektorov bankovníctvo, infraštruktúra finančných trhov a digitálna infraštruktúra. Pri identifikácii kritických subjektov členské štáty zohľadňujú **výsledky posúdenia rizík** a uplatňujú **tri (kumulatívne) 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.¹⁴²

Pri **určovaní závažnosti rušivého vplyvu** uvedeného v článku 5 ods. 2 písm. c) členské štáty zohľadňujú tieto **kritériá**:¹⁴³

- a) *počet používateľov využívajúcich službu, ktorú poskytuje subjekt;*
- b) *závislosť iných odvetví uvedených v prílohe od tejto služby;*
- c) *vplyv, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti, životné prostredie a verejnú bezpečnosť;*
- d) *trhový podiel subjektu na trhu s takýmito službami;*
- e) *geografická oblasť, ktorú by incident mohol ovplyvniť, vrátane akýchkoľvek cezhraničných vplyvov;*
- f) *význam subjektu z hľadiska zachovania dostatočnej úrovne služby berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby.*

Vyššie uvedené kritériá pre identifikáciu kritických subjektov do značnej miery vychádzajú z kritérií pre identifikáciu prevádzkovateľov základných služieb v zmysle čl. 5 ods. 2 Smernice NIS. Rozdielnosti možno vidieť najmä v tom, že Návrh smernice o odolnosti kritických prvkov v čl. 5 ods. 2

¹⁴¹ Klasifikácia NUTS rozčleňuje v zmysle nariadenia (ES) č. 1059/2003 hospodárske územie členských štátov na územné jednotky troch úrovní (NUTS 1, NUTS 2 a NUTS 3). Táto klasifikácia je doplnená o lokálne administratívne jednotky (LAU), ktoré predstavujú podrobnejšie členenie úrovne NUTS 3.

¹⁴² Návrh smernice o odolnosti kritických subjektov, článok 2.

¹⁴³ Návrh smernice o odolnosti kritických subjektov, článok 6.

písm. a) používa pojem základná služba a subjekt môže poskytovať aj viac ako len jednu takúto službu. Ďalšou odlišnosťou je skutočnosť, že poskytovanie základnej služby v zmysle čl. 5 ods. 2 písm. b) závisí od infraštruktúry a nie len sietí a informačných systémov. Odlišnosťou je aj textácia čl. 5 ods. 2 písm. c), kde je vyslovene uvedené, že incident môže mať závažný rušivý vplyv nie len na poskytovanie danej služby ale aj iných základných služieb v odvetviach uvedených v prílohe, ktoré závisia od služby.

Členské štáty sú povinné zostaviť **zoznam identifikovaných kritických subjektov**. Zoznam identifikovaných kritických subjektov je **preskúmaný** podľa potreby v každom prípade aspoň každé štyri roky a **v náležitých prípadoch môže byť aj aktualizovaný**.

Úloha pre MIRRI

Monitorovať transpozíciu prijatého Návrhu smernice o odolnosti kritických subjektov, a to najmä s ohľadom na správnu interpretáciu pojmu subjekt verejnej správy v rámci nového sektora Verejná správa, ako aj určovania prahových hodnôt v odvetví, resp. pododvetví, kde bude MIRRI príslušným orgánom.

2.2.8.2. Kybernetická bezpečnosť

Návrh smernice o odolnosti kritických subjektov sa týka fyzických hrozieb, ako napr. prírodné nebezpečenstvá (zemetrasenia, sopečné erupcie, záplavy, klimatické zmeny, sucho a pod.), hrozba z vnútra (infiltrovaný zamestnanec môže zneužiť prístupové práva a spôsobiť organizácii škodu) a pod. Avšak kritické subjekty budú musieť byť odolné aj voči kybernetickým hrozbám. Platí, že všetky subjekty identifikované ako kritické subjekty budú musieť plniť aj požiadavky Návrhu smernice NIS 2, čo zabezpečí komplexný prístup pri zabezpečení odolnosti kritických subjektov.

Návrh smernice o odolnosti kritických subjektov nestanovuje povinnosť prijať konkrétne opatrenia, ktoré majú kritické subjekty implementovať ale určuje, **aký výsledok má kritický subjekt dosiahnuť**.

Členské štáty zabezpečia, aby kritické subjekty prijali **vhodné a primerané technické a organizačné opatrenia na zabezpečenie svojej odolnosti** vrátane **opatrení** potrebných na:

- a) **predchádzanie vzniku incidentov**, a to aj prostredníctvom opatrení na znižovanie rizika katastrof a adaptáciu na zmenu klímy;
- b) **zabezpečenie primeranej fyzickej ochrany citlivých oblastí, zariadení a inej infraštruktúry** vrátane oplotenia, bariér, nástrojov a postupov monitorovania bezpečnostnej zóny, ako aj detekčného vybavenia a kontrol prístupu;
- c) **odolávanie incidentom a zmierňovanie ich následkov** vrátane vykonávania postupov a protokolov riadenia rizík a krízového riadenia a postupov spojených s bezpečnostnými varovaniami;
- d) **zotavenie sa z incidentov** vrátane opatrení na zabezpečenie kontinuity činností a identifikácie alternatívnych dodávateľských reťazcov;

- e) **zabezpečenie primeraného riadenia bezpečnosti zamestnancov**, a to aj stanovením kategórií pracovníkov vykonávajúcich kritické funkcie, stanovením prístupových práv k citlivým oblastiam, zariadeniam a inej infraštruktúre a k citlivým informáciám, ako aj určením osobitných kategórií zamestnancov so zreteľom na článok 12;
- f) **zvyšovanie informovanosti príslušných pracovníkov** o opatreniach uvedených v písmenách a) až e).

Konkrétnym opatrením, ktoré majú kritické subjekty realizovať je **zavedenie a uplatňovanie plánu odolnosti** alebo rovnocenného dokumentu či dokumentov, v ktorých podrobne opíšu. V prípade ak kritické subjekty prijali opatrenia v súlade s povinnosťami obsiahnutými v iných aktoch práva EÚ, ktoré sú relevantné aj pre opatrenia uvedené v Návrhu smernice o odolnosti kritických subjektov, opíšu tieto opatrenia aj v pláne odolnosti alebo v rovnocennom dokumente či dokumentoch.

Podrobné pravidlá spresňujúce niektoré alebo všetky opatrenia, ktoré sa majú prijať budú stanovené v **delegovanom akte**, ktorí príjme Komisia. Cieľom týchto delegovaných aktov je účinné a konzistentné uplatňovanie opatrení v súlade s cieľmi tejto smernice, pričom sa zohľadní akýkoľvek relevantný vývoj v oblasti rizík, technológií alebo poskytovania dotknutých služieb, ako aj všetky osobitosti týkajúce sa konkrétnych odvetví a typov subjektov.

Pre účely stanovenia potrebných technických a metodických špecifikácií týkajúcich sa uplatňovania opatrení príjme Komisia **vykonávacie akty**.

Návrh smernice o odolnosti kritických subjektov definuje pojem **incident** ako: „každá udalosť, ktorá môže narušiť alebo ktorá naruša prevádzku kritického subjektu.“¹⁴⁴ Návrh smernice o odolnosti kritických subjektov sa zameriava na tzv. fyzické incidenty, ktoré nemajú pôvod v kybernetickom priestore. Kritické subjekty sú povinné bez zbytočného odkladu oznamovať príslušnému orgánu **incidenty, ktoré významne narúšajú alebo môžu významne narušiť ich prevádzku**. Predmetné ustanovenie článku 13 nehovorí o tom, že následkom incidentu je narušenie poskytovania základnej služby ale narušenie prevádzky kritického subjektu. Avšak vzhľadom na ciele Návrhu smernice o odolnosti kritických subjektov možno vykladať toto ustanovenie v užšom slova zmysle, a teda išlo by o narušenie prevádzky kritického subjektu, ktoré by spôsobilo zároveň aj narušenie poskytovania základnej služby.

Z ustanovenia článku 13 vyplýva, že kritické subjekty neoznamujú všetky incidenty ale len tie, ktoré významne narúšajú alebo môžu narušiť ich prevádzku. S cieľom určiť závažnosť narušenia alebo potenciálneho narušenia prevádzky kritického subjektu vyplývajúceho z incidentu sa zohľadňujú **najmä tieto parametre**:

- a) *počet používateľov postihnutých narušením alebo potenciálnym narušením.*
- b) *trvanie narušenia alebo predpokladané trvanie potenciálneho narušenia,*
- c) *geografické územie ovplyvnené narušením alebo potenciálnym narušením.*

¹⁴⁴ Návrh smernice o odolnosti kritických subjektov, článok 2 ods. 3.

Úloha pre MIRRI

Monitorovať transpozíciu prijatého Návrhu smernice o odolnosti kritických subjektov, a to najmä s ohľadom na určenie parametrov pre určenie závažnosti narušenia prevádzky kritického subjektu.

3. PRÁVNÁ ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE

Oblasť kybernetickej bezpečnosti je na úrovni právneho poriadku Slovenskej republiky upravená viacerými právnymi predpismi. Z pohľadu právnej úpravy kybernetickej bezpečnosti v kontexte verejnej správy sú primárnymi právnymi predpismi ZoKB a ZoITVS. ZoKB je výsledkom transpozície Smernice NIS a je vykonávaný niekoľkými vyhláškami NBÚ.¹⁴⁵ ZoITVS upravuje špecificky kybernetickú bezpečnosť informačných technológií vo verejnej správe a je vykonávaný niekoľkými vyhláškami.¹⁴⁶

Medzi ďalšie právne predpisy, ktoré čiastkovo upravujú problematiku kybernetickej bezpečnosti možno zaradiť zákon č. 45/2011 Z. z. o kritickej infraštruktúre. Aspekty kybernetickej bezpečnosti možno nájsť taktiež v právnej úprave týkajúcej sa ochrany osobných údajov či bezpečnosti elektronických komunikačných sietí.¹⁴⁷

V tejto časti analýzy sa zameriame na základné inštitúty ZoKB a ZoITVS. Konkrétne dôjde k analýze predmetu a pôsobnosti právnej úpravy, základných pojmov, bezpečnostných opatrení, bezpečnostných incidentov, dozoru a dohľadu a sankcií. Na základe výsledkov analýzy dôjde k identifikovaniu základných problémov a budú formulované konkrétne návrhy riešení.

3.1. Predmet a pôsobnosť právnej úpravy

3.1.1. Zákon o kybernetickej bezpečnosti

Cieľom ZoKB je vytvoriť organizačnými, technickými a právnymi opatreniami prostredie, v rámci ktorého by bola kritická informačná a komunikačná infraštruktúra, ako aj vybrané informačné systémy a siete, chránené na dostatočnej úrovni pred rôznymi kybernetickými bezpečnostnými hrozbami, ktoré by mohli v konečnom dôsledku ohroziť riadne fungovanie dôležitých hospodárskych či spoločenských činností v štáte.

ZoKB upravuje:¹⁴⁸

- a) *organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,*
- b) *národnú stratégiu kybernetickej bezpečnosti,*
- c) *jednotný informačný systém kybernetickej bezpečnosti,*

¹⁴⁵ Vyhláška č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby)

Vyhláška č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

Vyhláška č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov

Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Vyhláška č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

¹⁴⁶ Z oblasti kybernetickej bezpečnosti je tou najdôležitejšou vyhláškou vyhláška č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

¹⁴⁷ Napr. zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a zákon č. 452/2021 Z. z. o elektronických komunikáciách.

¹⁴⁸ ZoKB, § 1.

- d) *organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu,*
- e) *postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,*
- f) *bezpečnostné opatrenia,*
- g) *systém zabezpečenia kybernetickej bezpečnosti,*
- h) *kontrolu nad dodržiavaním tohto zákona a audit.*

Vecná pôsobnosť ZoKB je vymedzená pozitívne aj negatívne. V zmysle **pozitívneho vymedzenia pôsobnosti** ZoKB ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.¹⁴⁹ V zmysle **negatívneho vymedzenia pôsobnosti** sa ZoKB nevzťahuje na konkrétne právne predpisy, resp. na požiadavky na kybernetickú bezpečnosť upravené v konkrétnych právnych predpisoch. ZoKB sa nevzťahuje na:¹⁵⁰

- a) *požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,*
- b) *osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,¹⁾*
- c) *ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,²⁾*
- d) *požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému podľa osobitných predpisov,³⁾ vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,⁴⁾ a ani na platobné systémy a na systémy zúčtovania a vyrovnania cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,⁵⁾*
- e) *požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,⁶⁾ ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona,*
- f) *osobitné predpisy.⁷⁾*

Nakol'ko ZoKB v zmysle § 2 ods. 1 ustanovuje len **minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti**, možno ho považovať za **lex generalis** v oblasti kybernetickej bezpečnosti. Nie je vylúčené, aby konkrétny subjekt plnil povinnosti v zmysle iného právneho predpisu, ktorý bude pre dané odvetvie špecificky upravovať požiadavky na bezpečnosť sietí a informačných systémov, za predpokladu, že tieto požiadavky majú aspoň rovnocenný účinok ako povinnosti stanovené v ZoKB. Takýto právny predpis by mal charakter **lex specialis** k ZoKB.

Z pohľadu **osobnej pôsobnosti** sú regulovanými subjektmi najmä prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb. V kontexte právnej úpravy kybernetickej bezpečnosti vo verejnej správe sa budeme v analýze venovať najmä prevádzkovateľom základných

¹⁴⁹ ZoKB, § 2 ods. 1.

¹⁵⁰ ZoKB, § 2 ods. 2.

služieb, nakoľko sú orgány verejnej moci za splnenia určitých podmienok považované za prevádzkovateľov základných služieb v zmysle ZoKB. Vzhľadom na predmet analýzy sa nebudeme venovať poskytovateľom digitálnych služieb, medzi ktoré patrí online trhovisko, internetový vyhľadávač a služby cloud computingu.

3.1.1.1. Základné služby a prevádzkovateľ základných služieb

ZoKB definuje pojem základná služba a v predmetnej definícii sú uvedené dva druhy základných služieb. V zmysle § 3 písm. l) ZoKB je **základnou službou** služba, ktorá je zaradená v zozname základných služieb a:

1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,¹⁵¹
2. je prvkom kritickej infraštruktúry.

V **prílohe č. 1** sú definované sektory, podsektory a prislúchajúce typy prevádzkovateľov služieb. Nakoľko Smernica NIS umožňuje členským štátom regulovať prevádzkovateľov základných služieb podľa **zásady minimálnej harmonizácie**, členské štáty si túto úpravu mohli rozšíriť i na ďalšie, smernicou neuvedené odvetvia. Slovenská republika pridala sektor verejná správa a v rámci tohto sektora boli vytvorené štyri podsektory, konkrétne bezpečnosť, informačné systémy verejnej správy, obrana a utajované skutočnosti. **Zodpovedným ústredným orgánom za podsektor informačné systémy verejnej správy je MIRRI.** Ako typy prevádzkovateľov služieb sú v podsektore informačné systémy verejnej správy uvedení správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy a správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry.

Sektor	Podsektor	Typ prevádzkovateľa služby	Ústredný orgán
10. Verejná správa	Informačné systémy verejnej správy	správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 275/2006 Z. z. podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby ¹⁵²	MIRRI
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú	

¹⁵¹ V ZoKB boli v porovnaní so sektormi upravenými v smernici NIS pridané sektory ako verejná správa, priemysel, pošta či elektronické komunikácie.

¹⁵² Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov bol zrušený ZoITVS.

		prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
--	--	--	--

3.1.1.2. Identifikácia prevádzkovateľov základných služieb

Ak prevádzkovateľ služby v sektore podľa prílohy č. 1 zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovananej služby podľa § 18, je povinný to oznámiť NBU do 30 dní odo dňa, keď prekročenie zistil, najneskôr však do 60 dní, odkedy k prekročeniu došlo.¹⁵³

V zmysle § 18 ZoKB sa **identifikačné kritériá** prevádzkovananej služby delia na:

- a) dopadové kritériá,
- b) špecifické sektorové kritériá.

Dopadové kritériá vychádzajú z čl. 6 Smernice NIS, ktorý upravuje faktory pre určenie závažnosti rušivého vplyvu. Podrobnosti o dopadových a špecifických sektorových kritériách pre základnú službu sú upravené vo vyhláške NBU č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovananej služby (kritériá základnej služby) (ďalej len „**vyhláška č. 164/2018 Z. z.**“). Je potrebné podotknúť, že európsky zákonodarcia v Smernici NIS určuje identifikačné kritériá prevádzkovateľov základných služieb a nie identifikačné kritériá prevádzkovananej služby, tak ako to upravuje §18 ZoKB a vyhláška č. 164/2018 Z. z. Podstata určenia prevádzkovateľa základných služieb je ich identifikácia a nie identifikácia základnej služby.

Dopadové kritériá v zmysle ZoKB podobne ako medziodvetvové faktory v zmysle Smernice NIS zohľadňujú najmä:

- a) **počet používateľov** využívajúcich základnú službu,
- b) **závislosť ostatných sektorov** podľa prílohy č. 1 od základnej služby,
- c) **vplyv**, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu,
- d) **trhový podiel** prevádzkovateľa služby,
- e) **geografické rozšírenie** z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť,
- f) **význam prevádzkovateľa základnej služby** z hľadiska **zachovania kontinuity** poskytovania služby.

V zmysle vyhlášky č. 164/2018 Z. z. prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, ak spĺňa **aspoň jedno dopadové kritérium a aspoň jedno špecifické sektorové kritérium**.¹⁵⁴

¹⁵³ ZoKB, § 17 ods. 1.

¹⁵⁴ Vyhláška č. 164/2018 Z. z., § 2.

V § 18 ods. 4 ZoKB je uvedené, že ak prevádzkovateľ služby podľa prílohy č. 1 ZoKB zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to NBÚ do 30 dní odo dňa, keď prekročenie zistil aj v prípade, ak neprekročí dopadové kritériá.

NBÚ zaradí základnú službu, ktorá závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, do **zoznamu základných služieb** a jej prevádzkovateľa do **registra PZS**:

- a) na základe **oznámenia** prevádzkovateľom tejto služby,
- b) na základe **podnetu** ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovej služby podľa § 18 ZoKB,
- c) **z vlastnej iniciatívy**, ak sa NBÚ dozvedel o prekročení identifikačných kritérií prevádzkovej služby podľa § 18 ZoKB a nedošlo k postupu podľa písmena a) alebo písmena b) ZoKB.¹⁵⁵

V prípade základných služieb, keď je služba ako **prvok kritickej infraštruktúry**, platí, že NBÚ zaradí takúto základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS zo zákona.¹⁵⁶

Zaradenie základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS **oznámi** NBÚ prevádzkovateľovi tejto služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.¹⁵⁷ NBÚ o zaradení nevydáva individuálny právny akt. Proti takémuto oznámeniu nie je možné podať opravné prostriedky v zmysle zákona č. 71/1967 Z. o správnom konaní (správny poriadok).¹⁵⁸

3.1.2. Zákon o informačných technológiách vo verejnej správe

ZoITVS upravuje:¹⁵⁹

- 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.*

V ustanoveniach ZoITVS, ktoré upravujú predmet a vecnú pôsobnosť právnej úpravy sa vyslovene neuvádza kybernetická bezpečnosť či bezpečnosť informačných technológií verejnej správy.

V zmysle § 1 ods. 3 ZoITVS sa na informačné technológie verejnej správy vzťahuje ZoKB ak ZoITVS v § 18 až 22 neustanovuje inak.

¹⁵⁵ ZoKB, § 17 ods. 2.

¹⁵⁶ ZoKB, § 17 ods. 3.

¹⁵⁷ ZoKB, § 17 ods. 5.

¹⁵⁸ ZoKB, § 33 ods. 1.

¹⁵⁹ ZoITVS, § 1 ods. 1.

V ustanovení § 18 ZoITVS sú základné ustanovenia týkajúce sa situácie, kedy je správca informačných technológií verejnej správy zároveň aj prevádzkovateľom základnej služby v zmysle ZoKB. Predmetný zákon upravuje bezpečnosť informačných technológií verejnej správy v oblasti:

- plánovania a organizácie (§ 19),
- obstarávania a implementácie (§ 20),
- prevádzky, servisu a podpory (§ 21),
- monitoringu a hodnotenia (§ 22),

V ustanovení § 23 predmetného zákona sú upravené osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy (napr. bezpečnostný projekt, hlásenie kybernetických bezpečnostných incidentov).

ZoITVS sa v rozsahu ustanovenom osobitnými predpismi vzťahuje aj na osoby, o ktorých to tieto osobitné predpisy ustanovia.¹⁶⁰

V zmysle negatívneho vymedzenia pôsobnosti sa ZoITVS nevzťahuje na informačné technológie verejnej správy, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, ochrany utajovaných skutočností a citlivých informácií.

V kontexte **osobnej pôsobnosti** sa ZoITVS v rámci organizácie správy informačných technológií verejnej správy vzťahuje na **orgán vedenia** a **orgány riadenia**. Orgánom vedenia je MIRRI.¹⁶¹ Orgánmi riadenia na účely ZoITVS sú:¹⁶²

- a) *ministerstvo a ostatný ústredný orgán štátnej správy,*
- b) *Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a iný štátny orgán,*
- c) *obec a vyšší územný celok,*
- d) *Kancelária Národnej rady Slovenskej republiky, Kancelária prezidenta Slovenskej republiky, Kancelária Ústavného súdu Slovenskej republiky, Kancelária Najvyššieho súdu Slovenskej republiky, Kancelária Najvyššieho správneho súdu Slovenskej republiky, Kancelária Súdnej rady Slovenskej republiky, Kancelária verejného ochrancu práv, Úrad komisára pre deti, Úrad komisára pre osoby so zdravotným postihnutím, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra Slovenskej republiky, Rozhlas a televízia Slovenska, Rada pre vysielanie a retransmisiu,*
- e) *právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),*

¹⁶⁰ ZoITVS, § 1 ods. 4. Napr. § 20 ods. 1 písm. j) zákona č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov, § 44a zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska.

¹⁶¹ ZoITVS, § 5 ods. 1 písm. a).

¹⁶² ZoITVS, § 5 ods. 2.

- f) komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,*
- g) osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,*
- h) záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.*

ZoITVS taktiež rozlišuje medzi správcom a prevádzkovateľom. Správcom je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. V prípade ak ZoITVS vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely ZoITVS ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby. Prevádzkovateľom je na účely ZoITVS správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba.¹⁶³

Povinnosť správcu zabezpečiť riadenie bezpečnosti je zakotvená v § 14 ods. 1 písm. i) ZoITVS. V súvislosti s bezpečnostnými opatreniami je správca povinný:

- určiť a zaviesť bezpečnostné opatrenia na procesnej, organizačnej a na technickej úrovni, (§ 19 ods. 1 písm. d) ZoITVS),
- určiť prostriedky a zdroje na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení, (§ 19 ods. 1 písm. e) ZoITVS),
- určiť prostriedky kontroly uplatňovania bezpečnostných opatrení, (§ 19 ods. 1 písm. f) ZoITVS),
- určiť postupy riešenia bezpečnostných incidentov, určiť prostriedky kontroly uplatňovania bezpečnostných opatrení, (§ 19 ods. 1 písm. g) ZoITVS),
- realizovať bezpečnostné opatrenia (§ 19 ods. 3 písm. c) zákona o ITVS).

3.1.2.1. Vzťah ZoKB a ZoITVS

Z pohľadu osobnej pôsobnosti ZoITVS a ZoKB môžu nastať situácie, že ten istý subjekt bude v postavení správcu podľa ZoITVS a prevádzkovateľa základnej služby podľa ZoKB. V tejto súvislosti bude pre takýto subjekt kľúčové, ktorý právny predpis má aplikovať pri prijímaní konkrétnych bezpečnostných opatrení a aké bezpečnostné opatrenia musí prijať a realizovať.

V zmysle § 18 ods. 1 ZoITVS je správca, ktorý je zároveň aj prevádzkovateľom základnej služby povinný prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov

¹⁶³ ZoITVS, § 2 ods. 5 a 6.

v zmysle § 20 ZoKB. Inými slovami, vo všeobecnosti platí, ak je správca aj prevádzkovateľ základných služieb v zmysle ZoKB, prijíma a realizuje bezpečnostné opatrenia v zmysle tohto právneho predpisu.

Avšak v zmysle § 18 ods. 2 ZoITVS správca, ktorý je prevádzkovateľom základnej služby v zmysle ZoKB, prijíma a realizuje bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe podľa ZoITVS a vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (ďalej len „**vyhláška č. 179/2020 Z. z.**“), ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje ZoKB. Inými slovami, subjekt, ktorý je v postavení správcu podľa ZoITVS a prevádzkovateľa základnej služby podľa ZoKB, bude musieť porovnávať bezpečnostné opatrenia v zmysle ZoITVS a ZoKB, resp. ich vyhlášiek. Ak správca dôjde k záveru, že cieľom bezpečnostných opatrení podľa ZoITVS a vyhlášky č. 179/2020 Z. z. je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje ZoKB, tak prijme a realizuje bezpečnostné opatrenia podľa ZoITVS a vyhlášky č. 179/2020 Z. z.

V súvislosti so vzťahom ZoKB a ZoITVS v kontexte realizácie bezpečnostných opatrení platí v zmysle § 2 ods. 3 vyhlášky č. 179/2020 Z. z., že ak sa aplikuje bezpečnostné opatrenie aj podľa ZoKB, aplikuje sa bezpečnostné opatrenie podľa ZoITVS, ak jeho cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa ZoKB.

3.1.3. Identifikované problémy a návrhy riešení

3.1.3.1. Zaradzovanie správcov do registra PZS v rozpore so smernicou NIS

K máju 2022 je v registri prevádzkovateľov základných služieb v sektore verejná správa a podsektore informačné systémy verejnej správy zaradených **1508** orgánov verejnej moci, ktorí sú správcami, resp. prevádzkovateľmi sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa ZoITVS. Tento vysoký počet prevádzkovateľov základných služieb možno odôvodniť najmä s ohľadom na predchádzajúcu právnu úpravu ZoKB. Podľa znenia ZoKB **účinného do 31.7.2021** definoval ZoKB základnú službu ako službu, ktorá je zaradená v zozname základných služieb a:

1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,
2. **je informačným systémom verejnej správy,**
3. je prvkom kritickej infraštruktúry.

Zaradzovanie informačného systému verejnej správy do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb vykonával NBÚ v spolupráci s príslušným ústredným orgánom, ktorým bol právny predchodca MIRRI, a teda Úrad podpredsedu vlády pre investície a informatizáciu.¹⁶⁴ Takýmto spôsobom bolo zaradených vyše 1300 správcov do registra PZS.

¹⁶⁴ § 17 ods. 3 ZoKB účinného do 31.7.2021.

Novelou ZoKB¹⁶⁵ bolo vypustené ustanovenie o informačných systémoch verejnej správy ako druhu základných služieb. Taktiež boli vypustené ustanovenia o zaradovaní informačných systémov verejnej správy do zoznamu základných služieb a ich prevádzkovateľov do registra PZS.

K vypusteniu týchto ustanovení došlo najmä z dôvodu, že **pri základných službách – informačný systém verejnej správy a ich prevádzkovateľoch sa neskúmali dopadové kritériá** v zmysle ZoKB a vyhlášky č. 164/2018 Z. z.

Predmetná vyhláška určuje identifikačné kritériá základnej služby, ktorá závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1 ZoKB. **Pri prevádzkovateľoch základných služieb, ktorí poskytovali základnú službu – informačný systém verejnej správy, sa nikdy neskúmalo naplnenie dopadových kritérií.** K tomuto záveru možno dospieť na základe toho, že vyhláška č. 164/2018 Z. z. sa vzťahuje len na základné služby podľa § 3 písm. k) prvého bodu ZoKB, avšak nie na základné služby § 3 písm. k) druhého bodu ZoKB (účinného k 31.7.2021). **Neskúmanie dopadových kritérií je v rozpore so Smernicou NIS**, konkrétne tretej podmienky, a teda aby mal incident závažný rušivý vplyv na poskytovanie služby, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.

V praktickej rovine však táto zmena ZoKB nepriniesla želaný výsledok, nakoľko tieto subjekty sú stále v registri PZS a ich služby v zozname základných služieb. Tento stav nastal z dôvodu, že **NBÚ zmenil typ identifikácie prevádzkovanej služby zaradenej do zoznamu základných služieb ako typ služby podľa § 3 písm. k) druhého bodu ZoKB (účinnom do 31.7.2021) na základnú službu zaradenú ako typ služby podľa § 3 písm. k) prvého bodu ZoKB (účinnom do 31.7.2021).** Zmena identifikácie prevádzkovanej základnej služby bola vykonaná oznámením, ktoré má formálny charakter a nezakladá žiadne zmeny v právach a povinnostiach prevádzkovateľa základnej služby. V tejto súvislosti je potrebné podotknúť, že **v zmysle ZoKB nemá NBÚ právomoc meniť typ identifikácie prevádzkovanej služby.**

Všetci prevádzkovatelia základných služieb, ktorých služba je zaradená do zoznamu základných služieb a jej prevádzkovateľ v registri prevádzkovateľov základných služieb v sektore verejná správa, podsektore informačné systémy verejnej správy a pri ktorých sa neskúmali dopadové kritériá by mali byť zo zoznamu a registra vyradení a malo by dôjsť k opätovnej identifikácii.

ZoKB neupravuje možnosť požiadať o vyradenie zo zoznamu základných služieb a z registra PZS z dôvodu, že subjekt nespĺňa dopadové kritériá. Avšak pri použití analógie so situáciou, kedy NBÚ zmenil typ identifikácie prevádzkovanej služby bez zákonného zmocnenia, môžeme konštatovať, že aj v prípade výmazu základnej služby zo zoznamu a prevádzkovateľa z registra PZS by mohol NBÚ tento úkon vykonať oznámením.

¹⁶⁵ Zákon č. 287/2021 Z. z. ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

Úloha pre MIRRI

Iniciovať vyradenie správcov, ktorí sú zaradení v registri PZS v sektore verejná správa a podsektore informačné systémy verejnej správy, pri ktorých sa neskúmali dopadové kritériá.

3.1.3.2. Neúplný zoznam orgánov riadenia vo vyhláske č. 179/2020 Z. z.

Vo vyhláske č. 179/2020 Z. z. sú v ustanovení § 3 uvedené tri kategórie bezpečnostných opatrení, ktoré majú spĺňať konkrétni správcovia. Zoznam správcov vychádza z ustanovenia § 5 ods. 2 ZoITVS, ktorý vymenúva orgány riadenia. Konkrétne ide o nasledujúce orgány riadenia:

Bezpečnostné opatrenia kategórie I sa vzťahujú na:

- obec do 6000 obyvateľov,
- obec so štatútom mesta do 6000 obyvateľov,
- právnickú osobu v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia podľa § 5 ods. 2 písm. a) až d) ZoITVS, ktorá nie je uvedená v odsekoch 3 a 4.

Bezpečnostné opatrenia kategórie I a II sa vzťahujú na:

- obec nad 6000 obyvateľov,
- obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,³⁾
- mestská časť s právnou subjektivitou,⁴⁾
- Kancelária verejného ochrancu práv,
- Úrad komisára pre deti,
- Úrad komisára pre osoby so zdravotným postihnutím,
- Rada pre vysielanie a retransmisiu,
- prevádzkovateľ základných služieb podľa osobitného predpisu,²⁾ ktorého siete a informačné systémy sú zaradené do Kategórie I alebo Kategórie II podľa osobitného predpisu¹⁾ neuvedeného v odseku 4.

Bezpečnostné opatrenia kategórie I, II a III sa vzťahujú na:

- obec, ktorá je aj krajským mestom,³⁾
- samosprávny kraj,
- ministerstvo a ostatný ústredný orgán štátnej správy,⁵⁾
- Úrad pre reguláciu sieťových odvetví,
- Úrad pre reguláciu elektronických komunikácií a poštových služieb,
- Najvyšší kontrolný úrad Slovenskej republiky,
- Úrad pre dohľad nad zdravotnou starostlivosťou,
- Úrad na ochranu osobných údajov Slovenskej republiky,
- Generálnu prokuratúru Slovenskej republiky,
- Dopravný úrad,

- Ústav pamäti národa,
- Tlačovú agentúru Slovenskej republiky,
- Rozhlas a televíziu Slovenska,
- Kancelária Súdnej rady Slovenskej republiky,
- Kancelária Najvyššieho súdu Slovenskej republiky,
- Kancelária Ústavného súdu Slovenskej republiky,
- Kancelária prezidenta Slovenskej republiky,
- Kancelária Národnej rady Slovenskej republiky,
- Finančné riaditeľstvo Slovenskej republiky,
- Národná agentúra pre sieťové a elektronické služby,
- Zbor väzenskej a justičnej stráže,
- DataCentrum Ministerstva financií Slovenskej republiky,
- DataCentrum elektronizácie územnej samosprávy Slovenska,
- Sociálna poisťovňa,
- zdravotná poisťovňa,
- Národné centrum zdravotníckych informácií,
- prevádzkovateľ základných služieb podľa osobitného predpisu,²⁾ ktorého siete a informačné systémy sú zaradené do Kategórie III podľa osobitného predpisu.¹⁾

Zoznam orgánov riadenia podľa ZoITVS môže byť dopĺňaný, čo dokazuje aj novela ZoITVS, ktorou bola do výpočtu orgánov riadenia doplnená Kancelária Najvyššieho súdu Slovenskej republiky. Avšak vyhláška č. 179/2020 Z. z. túto zmenu nereflektovala a v ustanovení § 3 predmetnej vyhlášky Kancelária Najvyššieho súdu Slovenskej republiky absentuje.

V tejto súvislosti je potrebné novelizovať vyhlášku č. 179/2020 Z. z., takým spôsobom, aby Kancelária Najvyššieho súdu Slovenskej republiky bola uvedená v ustanovení § 3 ods. 4 vyhlášky č. 179/2020 Z. z. Taktiež platí, že akákoľvek ďalšia zmena a doplnenie orgánov riadenia v ZoITVS sa musí prejavíť aj vo vyhláške č. 179/2020 Z. z.

Úloha pre MIRRI

Aktualizovať zoznam orgánov riadenia uvedená v ustanovení § 3 ods. 4 vyhlášky č. 179/2020 Z. z.

3.1.3.3. Zoznam základných služieb pre podsektor informačné systémy verejnej správy

Pri posudzovaní toho, či subjekt poskytuje služby, ktoré sú pre zachovanie rozhodujúcich spoločenských alebo hospodárskych činností zásadné, stačí v zmysle Smernice NIS preskúmať, či uvedený subjekt poskytuje službu, ktorá je zahrnutá do **zoznamu základných služieb**. Zoznam základných služieb by mal pre členské štáty slúžiť ako referenčný bod umožňujúci identifikáciu

prevádzkovateľov základných služieb. Jeho účelom je určiť typy základných služieb v ktoromkoľvek danom odvetví uvedenom v Smernici NIS.¹⁶⁶ Členské štáty sú povinné vytvoriť takýto zoznam.¹⁶⁷

V prípade Slovenskej republiky k dnešnému dňu **nebol vytvorený relevantný zoznam základných služieb pre sektor verejná správa a podsektor informačné systémy verejnej správy**, ktorý by slúžil ako referenčný bod umožňujúci identifikáciu PZS. **Za základnú službu v žiadnom prípade nemožno považovať správu a prevádzku sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa ZoITVS.** Taktiež **nemožno považovať za základné služby všetky služby verejnej správy, služby vo verejnom záujme a verejné služby**, a to najmä s odôvodnením, že nie všetky takéto služby majú zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.

Taktiež je potrebné poznamenať, že v jednotnom informačnom systéme kybernetickej bezpečnosti je pri sektore verejná správa, podsektore informačné systémy verejnej správy uvedená ako základná služba: „*správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.*“ Táto formulácia vychádza z prílohy č. 1 ZoKB, kde je pri sektore verejná správa, podsektore informačné systémy verejnej správy uvedené: „*správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy v pôsobnosti povinnej osoby podľa zákona č. 275/2006 Z. z. podporujúci služby verejnej správy, služby o verejnom záujme a verejné služby.*“ Zatiaľ, čo zrušený zákon č. 275/2006 Z. z. z pohľadu osobnej pôsobnosti definuje povinné osoby, **ZoITVS už nepozná pojem povinná osoba.**

Úloha pre MIRRI

Identifikovať základné služby pre sektor verejná správa a podsektor informačné systémy verejnej správy. Táto úloha dokonca priamo vyplýva z ustanovenia § 9 ods. 1 písm. f) ZoKB, v zmysle ktorého MIRRI v rozsahu svojej pôsobnosti pre sektor verejná správa a podsektor informačné systémy verejnej správy, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá NBÚ na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb.

3.2. Základné pojmy

ZoKB definuje základné pojmy, ktoré sú známe už z oblasti informačnej bezpečnosti ako dôvernosť, dostupnosť, integrita, riziko či hrozba. Taktiež sú prebrané niektoré definície pojmov zo smernice NIS ako napríklad sieť a informačný systém. Pojem bezpečnosť sietí a informačných systémov, ktorý definuje Smernica NIS, je v ZoKB označený ako kybernetická bezpečnosť.

¹⁶⁶ Smernica NIS, článok 5 ods. 2 písm. a) a body 19 a 23 preambuly.

¹⁶⁷ Smernica NIS, článok 5 ods. 3.

V nasledujúcej tabuľke uvádzame **porovnanie vybraných pojmov**, ktoré definuje, resp. používa ZoKB a ZoITVS.

	ZoKB	ZoITVS	Poznámka
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	Neobsahuje tento pojem.	ZoITVS neobsahuje definíciu pojmu kybernetická bezpečnosť. ZoITVS používa pojem bezpečnosť informačných technológií verejnej správy, avšak tento pojem nedefinuje.
Kybernetický bezpečnostný incident	kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je <ol style="list-style-type: none"> 1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, 2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, 3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo 4. ohrozenie bezpečnosti informácií, 	Obsahuje tento pojem, avšak ho nedefinuje.	ZoITVS v ustanovení § 23 ods. 3 písm. a) ZoITVS pri pojme kybernetický bezpečnostný incident odkazuje na ZoKB.
Bezpečnostné opatrenie	Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej a	Obsahuje tento pojem, avšak ho nedefinuje.	

	<p>technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifik kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti.</p>		
Bezpečnostná dokumentácia	<p>Obsah a štruktúra bezpečnostnej dokumentácie je upravená vo vyhláške č. 362/2018 Z. z.</p>	<p>Tento pojem používa ale nedefinuje.</p>	<p>ZoITVS ani príslušná vyhláška č. 179/2020 Z. z. špecificky neupravuje čo je obsahom a akú štruktúru má mať bezpečnostná dokumentácia. Tento pojem ZoITVS používa napr. v § 19 ods. 2 písm. a) a ods. 3 písm. a). Podľa § 23 ods. 1 ZoITVS je súčasťou bezpečnostnej</p>

			dokumentácie bezpečnostný projekt informačných systémov verejnej správy, ktorého obsah a štruktúra je špecificky upravená vo vyhláške č. 179/2020 Z. z.
Integrita, dôvernosť, dostupnosť	<p>Integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,</p> <p>Dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,</p> <p>Dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,</p>	Nedefinuje tieto pojmy.	Vyhláška č. 179/2020 Z. z. tieto pojmy používa, avšak nedefinuje.

Bezpečnostná dokumentácia podľa vyhlášky č. 362/2018 Z. z. obsahuje v § 2 ods. 1 výpočet obligatórnych obsahových prvkov. V ustanovení § 2 ods. 3 je tento výpočet doplnený o fakultatívne obsahové prvky. V nasledujúcej tabuľke uvádzame, čo je obsahom bezpečnostnej dokumentácie podľa ZoKB a vyhlášky č. 362/2018 Z. z. a následne obsahové prvky porovnáme s právnou úpravou v ZoITVS a príslušnej vyhláške.

ZoKB a vyhláška č. 362/2018 Z. z.	Poznámka	ZoITVS a vyhláška č. 179/2020 Z. z.	Poznámka
Bezpečnostná dokumentácia obsahuje:			
<ul style="list-style-type: none"> schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti, 	<p>Obsahové prvky bezpečnostnej stratégie kybernetickej bezpečnosti sú uvedené v § 3 vyhlášky č. 362/2018 Z. z. Štruktúra bezpečnostnej stratégie a bezpečnostnej politiky kybernetickej bezpečnosti je obsahom prílohy č. 1 k predmetnej vyhláške.</p>	<p>ZoITVS a vyhláška č. 179/2020 Z. z. používa pojem bezpečnostná stratégia kybernetickej bezpečnosti a bezpečnostné politiky.</p> <p>Obsahové prvky bezpečnostnej stratégie kybernetickej bezpečnosti nie sú upravené.</p> <p>Vyhláška č. 179/2020 Z. z. uvádza ako jedno z bezpečnostných opatrení v kategórii II: <i>„Vypracovanie a implementácia interného riadiaceho aktu</i> Politika kybernetickej bezpečnosti a informačnej</p>	<p>Podľa § 19 ods. 3 písm. a) ZoITVS správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti zabezpečuje vypracovanie a aktualizáciu bezpečnostnej dokumentácie upravujúcej systém riadenia bezpečnosti. Riadiaca zložka systému riadenia bezpečnosti zabezpečuje prerokovanie a schválenie bezpečnostnej stratégie kybernetickej bezpečnosti.</p> <p>Vo vyhláške č. 179/2020 Z. z. je uvedené, že manažér kybernetickej bezpečnosti a informačnej bezpečnosti pri výkone svojej činnosti navrhuje stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti a bezpečnostný výbor pri</p>

		<i>bezpečnosti, ktorý je pre organizáciu správcu záväzný...</i> " a definuje obsahové prvky tohto interného riadiaceho aktu.	výkone svojej činnosti riadi stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti.
<ul style="list-style-type: none"> klasifikáciu informácií a kategorizáciu sietí a informačných systémov, 	Štruktúra klasifikácie informácií a kategorizácie sietí a informačných systémov je obsahom prílohy č. 2 vyhlášky č. 362/2018 Z. z.	<p>Podľa ustanovenia § 11 ods. 4 ZoITVS sa na účely klasifikácie informácií a kategorizácie sietí a informačných systémov použijú ustanovenia ZoKB.</p> <p>Vyhláška č. 179/2020 Z. z. v zmysle § 1 ods. 1 písm. a) pre kategórie informačných technológií verejnej správy a pre podrobnosti o spôsobe zarad'ovania do týchto kategórií používa klasifikáciu informácií a kategorizácie sietí a informačných systémov podľa vyhlášky č. 362/2018 Z. z.</p>	
<ul style="list-style-type: none"> zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých 		Správca je v zmysle § 19 ods. 1 písm. d) ZoITVS povinný vo svojej organizácii zaviesť a udržiavať	V zmysle § 19 ods. 2 písm. c) ZoITVS správca prostredníctvom riadiacej zložky systému riadenia bezpečnosti zabezpečuje prerokovanie

<p>bezpečnostných opatrení; konkrétny obsah môže byť odvodený z princípov niektorého z rámcov riadenia bezpečnostnej architektúry,</p>		<p>systém riadenia informačnej bezpečnosti, ktorý určí a zavedie bezpečnostné opatrenia na procesnej, organizačnej a na technickej úrovni.</p> <p>Podľa prílohy č. 3 vyhlášky č. 179/2020 Z. z. bezpečnostný zámer ako výstup bezpečnostného projektu informačného systému verejnej správy obsahuje rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany informačného systému verejnej správy, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu, do ktorej je informačný systém verejnej správy zaradený.</p>	<p>a schválenie návrhu opatrení. Návrh vyplýva z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov kybernetickej bezpečnosti informačných technológií verejnej správy.</p> <p>Taktiež je v zmysle § 19 ods. 3 písm. c) správca prostredníctvom výkonnej zložky systému riadenia bezpečnosti povinný realizovať bezpečnostné opatrenia.</p>
--	--	--	---

<ul style="list-style-type: none"> vykonanú analýzu rizík kybernetickej bezpečnosti, 		<p>V zmysle vyhlášky č. 179/2020 Z. z. sa analýza rizík vykonáva v rámci vyhotovenia dokumentu analýza bezpečnosti. Tento dokument je hlavným výstupom bezpečnostného projektu informačného systému verejnej správy.</p>	
<ul style="list-style-type: none"> záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti 		<p>Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti sa vykonáva podľa vyhlášky Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.</p>	
<p>Bezpečnostná dokumentácia môže zahŕňať aj:</p>			
<ul style="list-style-type: none"> bezpečnostné štandardy, ktoré interpretujú požiadavky platných bezpečnostných 		<p>V zmysle prílohy č. 3 vyhlášky č. 179/2020 Z. z. obsahuje bezpečnostný zámer najmenej formuláciu základných</p>	

<p>politík v konkrétnych situáciách, určujú aktivity, hlavné pravidlá, zodpovednosti a organizáciu riadenia s cieľom podporiť dodržiavanie bezpečnostných politík</p>		<p>bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe.</p>	
<ul style="list-style-type: none"> • bezpečnostné návody, ktoré predstavujú súhrn predpísaných krokov na vykonanie bezpečnostných politík a bezpečnostných štandardov prostredníctvom konkrétnych akcií a ktoré opisujú bezpečnostné konfigurácie a poskytujú konkrétne, platformovo závislé usmernenia na podporu bezpečnostných 		<p>Vyhláška č. 179/2020 Z. z. v súvislosti s návodmi uvádza v § 1 ods. 4, že: <i>„Na splnenie požiadaviek zákona a tejto vyhlášky sa poskytnú správcovi súbor materiálov, ktorý obsahuje šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy, návody, školiace materiály a ukážky.“</i></p>	

politík a bezpečnostných štandardov.			
--------------------------------------	--	--	--

Hoci **ZoITVS a vyhláška č. 179/2020 Z. z. nedefinujú obsahové prvky bezpečnostnej dokumentácie**, špecificky upravuje **bezpečnostný projekt informačného systému verejnej správy**, jeho obsah a štruktúru.

Bezpečnostný projekt podľa ZoITVS a vyhlášky č. 179/2020 Z. z. pozostáva z dvoch hlavných výstupov:

Bezpečnostný zámer	<p>Určuje najmä kontext a zameranie bezpečnostného projektu, preto obsahuje najmenej:</p> <ul style="list-style-type: none">a) formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov orgánu riadenia, technických noriem a štandardov dobrej praxe,b) zoznam právnych predpisov aplikovaných v bezpečnostnom projekte, ako aj interných riadiacich aktov,c) metodický prístup ku kvalitatívnej analýze rizík, ktorá je v bezpečnostnom projekte vykonaná,d) rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany informačného systému verejnej správy, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu, do ktorej je informačný systém verejnej správy zaradený,e) vymedzenie okolia informačného systému verejnej správy a jeho vzťah k možnému narušeniu bezpečnosti informačného systému verejnej správy vrátane zoznamu integrácií na informačný systém verejnej správy,f) vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,g) ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu informačného systému verejnej správy),h) postupy revízie/aktualizácie bezpečnostného zámeru.
Analýza bezpečnosti	<p>Súčasťou analýzy bezpečnosti je kvalitatívna analýza rizík. Analýza rizík sa vykonáva pre informačný systém verejnej správy priebežne počas celého projektu v súlade so zákonom a priamo nadväzuje na dokument bezpečnostný zámer. Analýza rizík pozostáva z výkonu týchto činností:</p>

	<ul style="list-style-type: none"> a) vytvorenie podkladových katalógov na analyzované riziká určených na identifikáciu aktív, identifikáciu hrozieb a zraniteľností a identifikáciu vplyvov, b) identifikácia a opis analyzovaných rizík v štruktúre podľa oblastí ustanovených ZoKB alebo podľa technickej normy (Například STN EN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002) (36 9784). c) priradenie aktív, hrozieb, zraniteľností a vplyvov ku každému z identifikovaných rizík, d) identifikácia realizovaných bezpečnostných opatrení, e) vyhodnotenie rizík spôsobom kombinácie pravdepodobnosti realizácie scenáru rizika a závažnosti vplyvu, f) opis navrhovaných bezpečnostných opatrení.
--	--

3.2.1. Identifikované problémy a návrhy riešení

3.2.1.1. Pojem kybernetická bezpečnosť v kontexte ZoITVS

Ako vyplýva z vyššie uvedenej analýzy, ZoITVS nepoužíva pojem kybernetická bezpečnosť, avšak namiesto tohto pojmu používa pojem bezpečnosť informačných technológií verejnej správy. ZoITVS v prípade pojmu bezpečnosť informačných technológií verejnej správy neodkazuje na pojem kybernetická bezpečnosť podľa ZoKB. V tejto súvislosti je potrebné analyzovať či pojem kybernetická bezpečnosť podľa ZoKB je aplikovateľný aj na pojem bezpečnosť informačných technológií verejnej správy podľa ZoITVS.

Pri pojme kybernetická bezpečnosť podľa ZoKB si je potrebné uvedomiť, že tento pojem je výsledkom transpozície Smernice NIS, ktorá definuje pojem bezpečnosť sietí a informačných systémov. Smernica NIS definuje bezpečnosť sietí a informačných systémov ako: „*schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernú uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.*“¹⁶⁸

V tejto súvislosti je potrebné zodpovedať na **otázku či možno informačné technológie verejnej správy podľa ZoITVS považovať za siete a informačné systémy v zmysle smernice NIS a ZoKB**. V nasledujúcej tabuľke uvádzame porovnanie:

¹⁶⁸ Smernica NIS, článok 4 ods. 2.

Smernica NIS	ZoKB	ZoITVS
<p>sieť a informačný systém je:</p> <p>a) elektronická komunikačná sieť v zmysle článku 2 písm. a) smernice 2002/21/ES;</p> <p>b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie digitálnych údajov, alebo</p> <p>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;</p>	<p>a) sieťou elektronická komunikačná sieť podľa osobitného predpisu,⁸⁾</p> <p>b) informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,</p>	<p>Informačnou technológiou je na účely tohto zákona prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby.</p> <p>Informačnou technológiou verejnej správy je informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe.</p>

		<p>Informačným systémom je na účely tohto zákona funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.</p>
		<p>Informačným systémom verejnej správy je informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.</p>
		<p>Infraštruktúrou technologicko-komunikačné prostredie zabezpečujúce implementáciu a prevádzkovanie informačných systémov verejnej správy, poskytovanie a rozvoj elektronických služieb verejnej správy,</p>
		<p>Informačnou činnosťou získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov.</p>
		<p>Elektronickou službou verejnej správy elektronická komunikácia s orgánom riadenia pri vybavovaní podania, oznámenia, pri prístupe k informáciám a ich poskytovaní alebo pri účasti verejnosti na správe verejných vecí.</p>

Z vyššie uvedených definícií vyplýva, že **pojem informačná technológia verejnej správy by sme mohli zahrnúť pod pojem siete a informačné systémy** podľa Smernice NIS a ZoKB. Pojem informačné technológie verejnej správy dokonca obsahuje aj prvky, ktoré pojem siete a informačné systémy neobsahujú ako napr. informačná činnosť a elektronické služby.

Na druhej strane treba dodať, že siete a informačné systémy sú úzko naviazané na poskytovanie základnej služby. Jednou z troch kumulatívnych podmienok pre identifikáciu prevádzkovateľa základnej služby je podmienka, že poskytovanie tejto služby, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností, je závislé od sietí a informačných systémov.¹⁶⁹ Avšak účelom informačných technológií verejnej správy je podpora služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Za určitých okolností by sme mohli konkrétne služby verejnej správy, služby vo verejnom záujme alebo verejné služby považovať za základné služby v zmysle Smernice NIS a ZoKB, avšak relevantný zoznam základných služieb pre sektor verejná správa a podsektor informačné systémy verejnej správy absentuje.

Na základe vyššie uvedeného možno konštatovať, že pojem kybernetická bezpečnosť v zmysle Smernice NIS a ZoKB je aplikovateľná aj na bezpečnosť informačných technológií verejnej správy. Je na zváženie či by nebolo vhodné pojem bezpečnosť informačných technológií verejnej správy definovať v ZoITVS, resp. odkázať na pojem kybernetická bezpečnosť v zmysle ZoKB.

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe

Definovať pojem bezpečnosť informačných technológií verejnej správy definovať v ZoITVS, resp. odkázať na pojem kybernetická bezpečnosť v zmysle ZoKB.

3.2.1.2. Terminologické nedostatky

Z vyššie uvedenej analýzy je zrejmé, že terminológia jednotlivých dokumentov v oblasti kybernetickej bezpečnosti sú v zmysle ZoKB, vyhlášky č. 362/2018 Z. z. a ZoITVS, vyhlášky č. 179/2020 Z. z. nekompatibilné. Zatiaľ čo ZoKB a vyhláška č. 362/2018 Z. z. používa pojem bezpečnostná dokumentácia, ZoITVS a vyhláška č. 179/2020 Z. z. sa zameriava viac na bezpečnostný projekt. Pri analýze obsahových prvkov jednotlivých dokumentov sme dospeli k záveru, že hoci je v niektorých prípadoch použitá iná terminológia, čo do obsahových prvkov sú tieto dokumenty častokrát podobné. Pre zvýšenie právnej istoty najmä vo vzťahu k regulovaným subjektom, ktorí sú v dvoch právnych postaveniach (prevádzkovateľ základnej služby podľa ZoKB a správca podľa ZoITVS), však bude potrebné zjednotiť terminológiu a doplniť chýbajúce obsahové prvky niektorých dokumentov ako napr. bezpečnostná stratégia kybernetickej bezpečnosti, ktorú upravuje ZoITVS.

Ako problematické však možno vnímať aj skutočnosť, že pojmy použité v ZoITVS a vyhláške č. 179/2020 Z. z. ako napr. bezpečnostná stratégia kybernetickej bezpečnosti nie sú konzistentné ani v samotnom ZoITVS a vyhláške č. 179/2020 Z. z. Napr. v § 19 ods. 2 písm. a) ZoITVS sa používa

¹⁶⁹ Smernica NIS, článok 5 ods. 2 písm. b).

pojem bezpečnostná stratégia kybernetickej bezpečnosti a vo vyhláske č. 179/2020 Z. z. sa používa pojem stratégia v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti.

V prípade vyhlášky č. 179/2020 Z. z. bolo z pohľadu terminológie identifikovaných niekoľko problémov. V prvom rade predmetná vyhláška používa pojem kybernetická a informačná bezpečnosť. Len pre pripomenutie, samotný ZoITVS tieto pojmy nepoužíva a ani ZoKB nedefinuje pojem informačná bezpečnosť. Vyhláška č. 179/2020 Z. z. taktiež používa pojem manažér kybernetickej bezpečnosti a informačnej bezpečnosti. ZoKB a príslušná vyhláška používa pojem manažér kybernetickej bezpečnosti. Máme za to, že by bolo potrebné ustáliť používanie pojmu kybernetická bezpečnosť.

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe

Zjednotiť terminológiu a doplniť chýbajúce obsahové prvky niektorých dokumentov, ako napr. bezpečnostná stratégia kybernetickej bezpečnosti.

3.3. Bezpečnostné incidenty

3.3.1. Zákon o kybernetickej bezpečnosti

Prevádzkovateľ základnej služby je povinný bezodkladne hlásiť závažný kybernetický bezpečnostný incident.¹⁷⁰ V zmysle ZoKB sa závažné kybernetické bezpečnostné incidenty členia na kategórie prvého, druhého a tretieho stupňa. Stanovenie konkrétneho stupňa závisí od nasledujúcich faktorov:¹⁷¹

- a) počtu používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
- b) dĺžky trvania kybernetického bezpečnostného incidentu,
- c) geografického rozšírenia kybernetického bezpečnostného incidentu,
- d) stupňa narušenia fungovania základnej služby alebo digitálnej služby,
- e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.

Kybernetický bezpečnostný incident možno považovať za závažný kybernetický bezpečnostný incident, ak spĺňa aspoň jedno identifikačné kritérium pre kategóriu závažného kybernetického bezpečnostného incidentu.¹⁷² Presná špecifikácia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov je predmetom vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (ďalej len „**vyhláška č. 165/2018 Z. z.**“).

¹⁷⁰ ZoKB, § 19 ods. 6 písm. b) a § 24 ods.1.

¹⁷¹ ZoKB, § 24 ods. 2.

¹⁷² Vyhláška č. 165/2018 Z. z., § 1 ods. 2

Kybernetické bezpečnostné incidenty možno v zmysle ZoKB a vyhlášky č. 165/2018 Z. z. rozdeľovať na ukončené závažné kybernetické bezpečnostné incidenty a prebiehajúce závažné kybernetické bezpečnostné incidenty. V prípade ukončeného závažného bezpečnostného incidentu jeho účinky do momentu hlásenia už pominuli. O prebiehajúcich závažných kybernetických bezpečnostných incidentoch možno hovoriť vtedy, ak do okamihu hlásenia takéhoto incidentu nepominuli jeho účinky. V takomto prípade je prevádzkovateľ základnej služby povinný odoslať neúplné hlásenie závažného kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.¹⁷³

3.3.2. Zákon o informačných technológiách vo verejnej správe

ZoITVS používa pojmy kybernetický bezpečnostný incident, závažný kybernetický bezpečnostný incident a odkazuje v prípade týchto pojmov na ustanovenia ZoKB. V ustanovení § 23 ods. 3 písm. a) ZoITVS je upravená povinnosť hlásiť kybernetické bezpečnostné incidenty subjektmi, ktorí sú:

1. **v dvoch právnych postaveniach** (správca podľa ZoITVS a zároveň prevádzkovateľ základnej služby v zmysle ZoKB),
2. **len správcami podľa ZoITVS.**

Ad 1)

Orgán riadenia podľa § 5 ods. 2 písm. a) a b) ZoITVS a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti, ktorí sú zaradení do registra prevádzkovateľov základných služieb podľa ZoKB, sú povinní nahlasovať prostredníctvom jednotného informačného systému verejnej správy **aj kybernetický bezpečnostný incident, na ktorý sa nevzťahuje povinnosť nahlasovania podľa ZoKB.**

Subjekt, ktorý je zároveň aj prevádzkovateľom základnej služby v zmysle ZoKB, je v prvom rade povinný hlásiť závažné kybernetické bezpečnostné incidenty v zmysle ZoKB. Avšak v zmysle vyššie uvedeného je takýto subjekt povinný **hlásiť aj kybernetický bezpečnostný incident, na ktorý sa nevzťahuje povinnosť nahlasovania podľa ZoKB.** V tomto prípade ide o kybernetické bezpečnostné incidenty, ktoré nie sú závažné v zmysle ZoKB a príslušnej vyhlášky. Inými slovami pôjde o kybernetické bezpečnostné incidenty, pri ktorých neboli presiahnuté kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov v zmysle vyhlášky č. 165/2018 Z. z.

Z vyššie uvedeného vyplýva, že **správca, ktorý je zároveň aj prevádzkovateľom základnej služby** nahlasuje NBÚ prostredníctvom jednotného informačného systému kybernetickej bezpečnosti:

- **závažné kybernetické bezpečnostné incidenty v zmysle ZoKB,**

¹⁷³ ZoKB, § 24 ods. 5.

- **kybernetické bezpečnostné incidenty v zmysle ZoKB, ktoré nie sú závažné.**

Je otázne, prečo sa od subjektov, ktoré sú v dvoch právnych postaveniach (správca podľa ZoITVS a zároveň prevádzkovateľ základnej služby v zmysle ZoKB) požaduje nahlasovanie v zásade všetkých kybernetických bezpečnostných incidentov a od subjektov, ktorí sú len prevádzkovateľmi základných služieb v zmysle ZoKB, sa požaduje nahlasovanie len závažných kybernetických bezpečnostných incidentov.

Ad 2)

V prípade správcov, ktorí nie sú prevádzkovateľmi základnej služby v zmysle ZoKB platí, že sú povinní nahlasovať kybernetický bezpečnostný incident, ktorý nie je závažný orgánu vedenia ním určeným spôsobom. Orgánom vedenia je MIRRI a za určený spôsob možno považovať nahlasovanie incidentov prostredníctvom Vládnej jednotky CSIRT.¹⁷⁴

3.3.3. Identifikované problémy a návrhy riešení

3.3.3.1. Kybernetické bezpečnostné incidenty, ktoré nie sú závažné

Ako už bolo uvedené vyššie, správca, ktorý je zároveň aj prevádzkovateľom základnej služby nahlasuje kybernetické bezpečnostné incidenty, ktoré nie sú závažné. V prípade správcu, ktorý nie je prevádzkovateľom základnej služby, nahlasuje takýto nezávažný kybernetický bezpečnostný incident Vládnej jednotke CSIRT.

V tejto súvislosti však vzniká otázka či **je možné pojem kybernetický bezpečnostný incident definovaný v ZoKB aplikovať aj pre účely ZoITVS**. Taktiež je otázne, **akým spôsobom vykladať kybernetické bezpečnostné incidenty, pri ktorých neboli presiahnuté kritériá** pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov v zmysle vyhlášky č. 165/2018 Z. z.

ZoKB v ustanovení § 3 písm. k) definuje kybernetický bezpečnostný incident ako: *„akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je*

1. *strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,*
2. *obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,*
3. *vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo*
4. *ohrozenie bezpečnosti informácií,*"

V zmysle vyhlášky č. 165/2018 Z. z. je kybernetický bezpečnostný incident identifikovaný ako závažný kybernetický bezpečnostný incident, **ak spĺňa aspoň jedno identifikačné kritérium pre**

¹⁷⁴ <https://www.csirt.gov.sk/nahlasit-incident.html?csrt=12716323446558195517>.

kategóriu závažného kybernetického bezpečnostného incidentu. Na základe uvedeného možno konštatovať, že **za kybernetický bezpečnostný incident, ktorý nie je závažný možno považovať kybernetický bezpečnostný incident v zmysle definície tohto pojmu podľa ustanovenia § 3 písm. k) ZoKB.**

Avšak pri bližšej analýze zistíme, že pojem kybernetický bezpečnostný incident nadväzuje na pojmy, ktoré nesúvisia s bezpečnosťou informačných technológií verejnej správy v zmysle ZoITVS a sú taktiež naviazané na základné služby.

V prvom rade v ZoKB sa za kybernetický bezpečnostný incident považuje: „*akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo **záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo***“ ZoITVS nedefinuje záväznú metodiku.

V druhom rade sa za kybernetický bezpečnostný incident považuje „*akákoľvek udalosť.....ktorej **následkom je***

2. *obmedzenie alebo odmietnutie **dostupnosti základnej služby alebo digitálnej služby,***
3. *vysoká pravdepodobnosť **kompromitácie činností základnej služby alebo digitálnej služby alebo***

Na kybernetické bezpečnostné incidenty, ktoré nie sú závažné taktiež nemožno v prípade **správcu, ktorý nie je prevádzkovateľom základnej** služby aplikovať bod 2 a 3 predmetnej definície pojmu kybernetický bezpečnostný incident, a to z toho dôvodu, že **v prípade ZoITVS sa neaplikujú základné služby a digitálne služby.**

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe

Zadefinovať pojem kybernetický bezpečnostný incident pre účely nahlasovania takýchto incidentov správcami, ktorí sú len v jednom právnom postavení.

3.3.3.2. Chýbajúca lehota

V prípade nahlasovania kybernetických bezpečnostných incidentov, ktoré nie sú závažné, správcami v jednom právnom postavení v zmysle ZoITVS absentuje lehota na nahlasovanie takýchto incidentov.

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe

Stanoviť lehotu na nahlasovanie kybernetických bezpečnostných incidentov, ktoré nie sú závažné na bezodkladne.

3.3.3.3. Rozšírenie osobnej pôsobnosti správcov, ktorí nahlasujú kybernetické bezpečnostné incidenty podľa ZoITVS

V aktuálnom účinnom znení ZoITVS sú v zmysle § 23 ods. 3 ZoITVS povinní nahlasovať kybernetické bezpečnostné incidenty títo správcovia (v jednom právnom postavení): „*Orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti.*”

Orgánmi riadenia podľa § 5 ods. 2 písm. a) ZoITVS sú: ministerstvo a ostatný ústredný orgán štátnej správy.

Orgánmi riadenia podľa § 5 ods. 2 písm. b) ZoITVS sú: Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a iný štátny orgán.

Osobnú pôsobnosť správcov by bolo v tomto prípade potrebné rozšíriť aj na ostatné orgány riadenia podľa § 5 ods. 2 písm. c) – h) ZoITVS.

Uvedený legislatívny nedostatok nemá za následok to, že napr. obce ako orgány riadenia podľa § 5 ods. 2 písm. c) ZoITVS nie sú povinné nahlasovať kybernetické bezpečnostné incidenty. Toto tvrdenie možno podporiť inými ustanoveniami ZoITVS, v zmysle ktorých sú správcovia povinní koordinovať riešenie bezpečnostných incidentov (§ 19 ods. 3 písm. e) ZoITVS) a taktiež sú povinní zabezpečiť realizáciu bezpečnostných opatrení (§ 19 ods. 3 písm. c) ZoITVS), medzi ktoré v zmysle vyhlášky č. 179/2020 Z. z. možno zaradiť aj hlásenie kybernetických bezpečnostných incidentov.

Avšak pre zlepšenie princípu právnej istoty by bolo vhodné doplniť rozsah osobnej pôsobnosti aj na orgány riadenia podľa § 5 ods. 2 písm. c) – h) ZoITVS.

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe

Rozšíriť povinnosť nahlasovať kybernetické bezpečnostné incidenty aj na orgány riadenia podľa § 5 ods. 2 písm. c) – h) ZoITVS.

3.4. Bezpečnostné opatrenia

V rámci tejto časti analýzy sa sústredíme na konkrétne bezpečnostné opatrenia vyžadované podľa ZoKB a ZoITVS. Nakoľko je problematika bezpečnostných opatrení pomerne rozsiahla, primárne sa budeme venovať ich komparácii a legislatívnemu vymedzeniu v ZoKB a ZoITVS. V prvých dvoch podkapitolách (3.4.1 a 3.4.2) uvedieme právnu úpravu bezpečnostných opatrení a ich rámcové vymedzenie. Kľúčovú časť predstavuje záverečná stať (3.4.3) kde v súhrnnej tabuľke uvádzame totožné a rozdielne bezpečnostné opatrenia podľa ZoKB a ZoITVS. Ako východiskový štandard

používame ZoKB, nakoľko práve táto právna úprava bola prijatá ako prvá a je transpozíciou Smernice NIS.

3.4.1. Zákon o kybernetickej bezpečnosti

ZoKB upravuje bezpečnostné pre prevádzkovateľov základných služieb v § 20. Tieto definuje ako „procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.“¹⁷⁵ Typ bezpečnostných opatrení výrazne závisí od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifik kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti. Rozsah pôsobnosti určuje Príloha č. 1 ZoKB. Špecifikáciu bezpečnostných opatrení upravuje vyhláška NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

§ 20 ZoKB ods. 3 definuje bezpečnostné opatrenia pre nasledujúce oblasti:

- 1) organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
- 2) riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- 3) personálna bezpečnosť,
- 4) riadenie prístupov,
- 5) riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- 6) bezpečnosť pri prevádzke informačných systémov a sietí,
- 7) hodnotenie zraniteľností a bezpečnostných aktualizácií,
- 8) ochrana proti škodlivému kódu,
- 9) sieťová a komunikačná bezpečnosť,
- 10) akvizícia, vývoj a údržba informačných sietí a informačných systémov,
- 11) zaznamenávanie udalostí a monitorovanie,
- 12) fyzická bezpečnosť a bezpečnosť prostredia,
- 13) riešenie kybernetických bezpečnostných incidentov,
- 14) kryptografické opatrenia,
- 15) kontinuita prevádzky,
- 16) audit, riadenie súladu a kontrolných činností.

Poskytovateľ digitálnej služby špecifické bezpečnostné opatrenia v ZoKB upravené nemá. Je to z toho dôvodu, že ich určuje vykonávacie nariadenie Európskej komisie.¹⁷⁶

¹⁷⁵ ZoKB, § 20 ods. 1.

¹⁷⁶ Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie tohto, či má incident závažný vplyv (Ú. v. EÚ L 26, 31. 1. 2018).

3.4.2. Zákon o informačných technológiách vo verejnej správe

Podobne, ako pri ZoKB, aj ZoITVS upravuje bezpečnostné opatrenia prostredníctvom zákonnej a podzákonnej právnej úpravy. Bezpečnostné opatrenia sú povinní prijať a realizovať správcovia. ZoITVS delí bezpečnostné opatrenia do nasledujúcich oblastí:

- 1) Bezpečnosť informačných technológií verejnej správy v oblasti plánovania a organizácie,
- 2) Bezpečnosť informačných technológií verejnej správy v oblasti obstarávania a implementácie,
- 3) Bezpečnosť informačných technológií verejnej správy v oblasti prevádzky, servisu a podpory,
- 4) Bezpečnosť informačných technológií verejnej správy v oblasti monitoringu a hodnotenia,
- 5) Osobitné opatrenia na úseku bezpečnosti informačných technológií verejnej správy.

Podrobná špecifikácia bezpečnostných opatrení sa nachádza vo vyhláške Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. V zmysle predmetnej vyhlášky sú upravené nasledovné oblasti:

- 1) organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
- 2) riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- 3) personálna bezpečnosť,
- 4) riadenie prístupov,
- 5) riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami,
- 6) bezpečnosť pri prevádzke informačných systémov a sietí,
- 7) hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
- 8) ochrana proti škodlivému kódu,
- 9) sieťová a komunikačná bezpečnosť,
- 10) akvizícia, vývoj a údržba informačných technológií verejnej správy,
- 11) zaznamenávanie udalostí a monitorovanie,
- 12) riadenie kontinuity procesov. fyzická bezpečnosť a bezpečnosť prostredia,
- 13) riešenie kybernetických bezpečnostných incidentov,
- 14) kryptografické opatrenia,
- 15) kontinuita prevádzky informačných technológií verejnej správy,
- 16) audit a kontrolné činnosti. audit, riadenie súladu a kontrolných činností.

3.4.3. Porovnanie bezpečnostných opatrení

V nasledujúcej tabuľke uvádzame rámcové porovnanie bezpečnostných opatrení v rámci oblastí kybernetickej a informačnej bezpečnosti v zmysle ZoKB, vyhlášky č. 362/2018 Z. z. a ZoITVS, vyhlášky č. 179/2020 Z. z.

Oblasť	ZoKB a vyhláška č. 362/2018 Z. z.	ZoITVS a vyhláška č. 179/2020 Z. z.	Poznámka
Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	<p>Na účely organizácie kybernetickej bezpečnosti sa uplatňuje najmenej zásada:</p> <ul style="list-style-type: none"> - Určenia manažéra kybernetickej bezpečnosti, - Najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh, - Oddel'ovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity, - Dodržiavania a vykonávania nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrovanie rizík, 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, - Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre organizáciu správcu záväzný a obsahuje konkrétne náležitosti. <p>Kategória II</p> <ul style="list-style-type: none"> - Vypracovanie a implementácia interného riadiaceho aktu Politika kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý je pre organizáciu správcu záväzný a obsahuje konkrétne náležitosti, - Určenie a personálne zabezpečenie roly manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu zodpovedného za koordináciu a plnenie konkrétnych úloh, 	<p>Vyhláška č. 179/2020 Z. z. popri manažérovi kybernetickej bezpečnosti upravuje aj iné osoby v oblasti kybernetickej bezpečnosti, konkrétne:</p> <ul style="list-style-type: none"> - pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, - bezpečnostný výbor. <p>Správca si určí pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti. Povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti budú upravené v internom riadiacom akte, ktorý prijme správca.</p>

	<ul style="list-style-type: none"> - Jasného vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností. 	<ul style="list-style-type: none"> - Vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej bezpečnosti a informačnej bezpečnosti v rozsahu a detaile zodpovedajúcom veľkosti a štruktúre organizácie správcu, významu informačných technológií verejnej správy v jeho správe a štruktúre existujúcich interných riadiacich aktov s detailným opisom jednotlivých opatrení a postupov pre konkrétne oblasti. <p>Kategória III</p> <ul style="list-style-type: none"> - Vytvorenie bezpečnostného výboru s rozsahom povinností a právomocí určených štatútom, - Vytvorenie pozície manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu mimo organizačného útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy, - Manažér kybernetickej bezpečnosti a informačnej bezpečnosti pri výkone svojej činnosti plní konkrétne úlohy, 	<p>Vyhláška č. 179/2020 Z. z. nedefinuje konkrétne povinnosti, zodpovednosti a právomoci.</p> <p>Úlohy manažéra kybernetickej bezpečnosti a informačnej bezpečnosti sú uvedené v prílohe č. 2 vyhlášky č. 179/2020 (Kategória II, písm. b), bod 1 – 10 a Kategória III, písm. e) bod 1 – 4).</p> <p>Bezpečnostný výbor plní konkrétne úlohy, ktoré sú uvedené v prílohe č. 2 vyhlášky č. 179/2020 (Kategória III, písm. b) bod 1 – 5).</p>
--	---	---	--

		<ul style="list-style-type: none"> - Zabezpečenie kontinuálneho vzdelávania manažéra kybernetickej bezpečnosti a informačnej bezpečnosti, - Uplatňovanie princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie správcu tak, že rovnaká osoba nie je zodpovedná za vykonávanie a zároveň aj schvaľovanie alebo kontrolu bezpečnostne relevantných aktivít a činností, - Zabezpečenie preskúmania a identifikácie bezpečnostných rizík v počiatočných fázach procesu riadenia projektov v organizácii správcu a určenie adekvátnych opatrení na zníženie každého identifikovaného rizika na prijateľnú úroveň. Definovanie osoby zodpovednej za kybernetickú a informačnú bezpečnosť v projektovom tíme, - Zabezpečenie vypracovania bezpečnostného projektu informačného systému verejnej správy. 	
Riadenie rizík kybernetickej bezpečnosti a	Bezpečnostné opatrenia v tejto oblasti upravujú:	Bezpečnostné opatrenia v tejto oblasti upravujú: Kategória I	Vyhláška č. 179/2020 Z. z. obsahuje v prílohe č. 1 zoznam aktív.

informačnej bezpečnosti	<ul style="list-style-type: none"> - Všetky aktíva súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami sú identifikované a inventár týchto aktív je centrálne zaznamenaný a riadený, - Riadenie aktív, - Ukončením pracovného pomeru alebo iného obdobného pracovného vzťahu zamestnancov prevádzkovateľa základnej služby a zamestnancov tretích strán sa zadokumentovaným spôsobom vracajú späť všetky zverené aktíva, - Riadenie rizík pozostáva z: <ul style="list-style-type: none"> • identifikácie zraniteľností, • identifikácie hrozieb, • identifikácie a analýzy rizík s ohľadom na aktívum, • určenia vlastníka rizika, • implementácie organizačných a technických bezpečnostných 	<ul style="list-style-type: none"> - Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti: • Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti. • Návrh a prijatie bezpečnostných opatrení. • Periodické preskúmavanie rizík. <p>Kategória II</p> <ul style="list-style-type: none"> - Identifikácia všetkých významných informačných aktív v organizácii správcu a určenie ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu. - Zaradenie informačných aktív podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných stupňov, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu. - Klasifikačné stupne pre informačné aktíva ustanovuje vyhláška č. 362/2018 Z. z. 	
--------------------------------	--	--	--

	<p>opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením,</p> <ul style="list-style-type: none"> • analýzy funkčného dopadu a • pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení. <p>- Súčasťou riadenia aktív, hrozieb a rizík je aj analýza funkčného dopadu, ktorá pozostáva z hodnotenia dopadu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby a spôsobiť ohrozenie alebo narušenie</p>	<ul style="list-style-type: none"> - Vypracovanie a implementácia interného riadiaceho aktu na riadenie bezpečnostných rizík, ktorý obsahuje najmenej: <ul style="list-style-type: none"> • zodpovednosť za vykonanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti, • proces vykonávania analýzy rizík, • maticu určenia závažnosti rizika, • periodicitu vykonávania analýzy rizík, • spôsob dokumentácie bezpečnostných rizík a prijatých opatrení a postupov na ich zníženie na prijateľnú úroveň v podľa matice určenia závažnosti rizika. - Vykonávanie analýzy rizík najmenej raz za dva roky. <p>Kategória III</p> <ul style="list-style-type: none"> - Vytvorenie a udržiavanie zoznamu informačných aktív každého organizačného útvaru organizácie správcu, ktorý je zároveň ich vlastníkom a ktorý určí požiadavky na 	
--	---	---	--

	kontinuity jeho poskytovanej základnej služby.	dôvernosť, dostupnosť a integritu každého informačného aktíva v jeho vlastníctve, - Vykonávanie analýzy rizík a vyhodnocovanie súladu implementovaných opatrení s touto vyhláškou najmenej raz ročne.	
Personálna bezpečnosť	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - Postupy pri zaradení osoby do niektorých z bezpečnostných rolí, presunu práv, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu, - Zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania spočívajúceho v oboznámení používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov s bezpečnostnými politikami a v pravidelnom zvyšovaní ich bezpečnostného 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Ustanoviť plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení a vykonať bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky. - Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia. - Zamestnávateľ povinnej osoby a tretia strana zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to 	<p>Vyhláška č. 179/2020 Z. z. je viac špecifickejšia, čo do rozvoja bezpečnostného povedomia, jeho hodnotenia, ako aj postupov oboznamovania sa s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.</p>

	<p>povedomia počas trvania pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,</p> <ul style="list-style-type: none"> - Kontrola dodržiavania bezpečnostných politík zo strany zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov, - Hodnotenie účinnosti plánu rozvoja bezpečnostného povedomia zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov, - Určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky zo strany používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov, 	<p>predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.</p> <ul style="list-style-type: none"> - Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti. - Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečia konkrétne požiadavky. - Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly. - Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu. 	
--	---	--	--

	<ul style="list-style-type: none"> - Postupy pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí umožňujúcich presun práv, povinností a zodpovedností na inú novú osobu, - Postupy pri porušení bezpečnostných politík spočívajúcich v oprávnení obmedziť alebo odňať prístupové oprávnenia a privilégiá, - Vykonalie poučenia o manipulácii s informáciami pre osoby, ktoré vykonávajú činnosť alebo sa oboznamujú s informáciami podľa §14b zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve. 	Kategória II <ul style="list-style-type: none"> - Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov, - Zavedenie procesu preukázateľného poučenia a oboznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti, - Zavedenie procesu preukázateľného oboznámenia správcov informačných technológií verejnej správy s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti, - Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oboznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, ako aj opatreniami 	
--	--	---	--

		<p>a postupmi zavedenými v organizácii správcu na ich elimináciu najmenej raz za dva roky.</p> <ul style="list-style-type: none"> - Na prístup k informačným technológiám verejnej správy sa vyžaduje: <ul style="list-style-type: none"> • oboznámenie so spôsobom používania informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy v rozsahu svojej pracovnej náplne, • poučenie na rozoznanie kybernetického bezpečnostného incidentu od bežnej prevádzky a zvládnutie postupu pri kybernetickom bezpečnostnom incidente, • oboznámenie so zamestnancom, na ktorého je možné sa obracať s otázkami a nejasnosťami pri používaní informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy. <p>Kategória III</p> <ul style="list-style-type: none"> - Vytvorenie evidencie informačných technológií verejnej správy s 	
--	--	--	--

		<p>priradením konkrétnych správcov, ktorí sú zodpovední za implementáciu a prevádzku bezpečnostných opatrení a postupov.</p> <ul style="list-style-type: none"> - Systematické zvyšovanie bezpečnostného povedomia tak, že pokrýva všetky oblasti ustanovené touto vyhláškou, ZoITVS, ZoKB a GDPR a najnovšími poznatkami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti v rozsahu pracovného zaradenia najmenej raz ročne. 	
Riadenie prístupov	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - Riadenie prístupov osôb k sieti a informačnému systému je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií verejnej správy, - Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy, - Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok. 	

	<p>a informačného systému, ktoré definujú spôsob pridelovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému,</p> <ul style="list-style-type: none"> - Riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou, 	<p>Kategória II</p> <ul style="list-style-type: none"> - Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií verejnej správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh, - Určenie postupu a zodpovednosti v súvislosti s pridelovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív, - Zaznamenávanie zmien v pridelenom prístupe a ich archivácia, - Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu, - Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá spĺňa konkrétne požiadavky, - Zabezpečenie formálneho riadenia a autorizácie pridelovania privilegovaných prístupov do informačných technológií 	
--	--	---	--

	<ul style="list-style-type: none"> - Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmenej: • vypracovanie zásad riadenia prístupu k informáciám, • riadenie prístupu používateľov, • zodpovednosť používateľov, • riadenie prístupu k sieťam, • prístup k operačnému systému a jeho službám, • prístup k aplikáciám, • monitorovanie prístupu a používania informačného systému a • riadenie vzdialeného prístupu. - V rámci riadenia prístupov k sieťam sú definované ďalšie požiadavky. 	<p>verejnej správy a ich obmedzenie len na nevyhnutné prípady,</p> <ul style="list-style-type: none"> - Preskúvanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za rok, - Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií verejnej správy a na prácu na diaľku. - Automatické zaznamenávanie každého prístupu administrátora do informačných technológií verejnej správy a automatické zaznamenávanie prístupu používateľa, - Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií verejnej správy. <p>Kategória III</p> <ul style="list-style-type: none"> - Implementácia centrálnej správy identít (IDM), - Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok, 	
--	--	--	--

		<ul style="list-style-type: none"> - Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť mesiacov, - Implementácia, vynucovanie prístupových rolí v informačných technológiách verejnej správy, - Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov šesť mesiacov, - Používanie silných autentizačných metód na overenie identity používateľov, ako je viacfaktorová autentizácia pri informačných technológiách verejnej správy, ktoré obsahujú prísne chránené informačné aktíva v zmysle klasifikácie informačných aktív. 	
Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo	Bezpečnostné opatrenia v tejto oblasti upravujú: <ul style="list-style-type: none"> - Na riadenie dodávateľských služieb, akvizície, vývoja a 	Bezpečnostné opatrenia v tejto oblasti upravujú: Kategória I <ul style="list-style-type: none"> - V zmluve s dodávateľmi musí byť určená požiadavka na dodržiavanie 	Zmluva s tretou stranou v zmysle vyhlášky č. 362/2018 Z. z. je čo do obsahových náležitostí špecifickejšia ako zmluva

<p>vzťahoch s tretími stranami</p>	<p>údržby informačných systémov sa pri uzatvorení zmluvy s tretou stranou analyzujú riziká dodávateľských služieb, akvizície, vývoja a údržby informačných systémov spôsobom,</p> <ul style="list-style-type: none"> - Zmluva s tretou stranou obsahuje konkrétne náležitosti, - Zmluva s tretou stranou obsahuje bezpečnostné opatrenia najmenej pre oblasť podľa § 20 ods. 3 písm. e), f), h), j) a k) ZoKB, - Vývoj a akvizícia siete a informačného systému základnej služby sa uskutočňuje s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v bezpečnostnej stratégii. 	<p>všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti. Môže byť uvedený odkaz na ZoITVS, túto vyhlášku alebo na GDPR.</p> <p>Kategória II</p> <ul style="list-style-type: none"> - Požiadavky v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií verejnej správy, - Zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahujú konkrétne náležitosti. - Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti a posúdia sa konkrétne aspekty, 	<p>s dodávateľmi podľa vyhlášky č. 179/2020 Z. z.</p>
---	---	---	---

	<ul style="list-style-type: none"> - Evidencia všetkých uzatvorených zmlúv s treťou stranou je súčasťou bezpečnostnej dokumentácie. 	<ul style="list-style-type: none"> - Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti, - Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu, - Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek. <p>Kategória III</p> <ul style="list-style-type: none"> - Pre informačné technológie verejnej správy, ktoré spracúvajú kritické informačné aktíva v 	
--	--	--	--

		<p>zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.</p> <ul style="list-style-type: none"> - Interný predpis ustanovujúci zásady kybernetickej bezpečnosti a informačnej bezpečnosti pre dodávateľov a tretie strany obsahuje konkrétne bezpečnostné požiadavky, - Vytvorenie a využívanie procesu pravidelného monitorovania a preskúmavania kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s dodávateľmi. 	
<p>Bezpečnosť pri prevádzke informačných systémov a sietí</p>	<p>Riadenie bezpečnosti sietí a informačných systémov sa zabezpečuje najmenej:</p> <ul style="list-style-type: none"> - riadením prístupov používateľov k sieťam a informačným systémom, - prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, a to 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Na účinnú prevenciu pred stratou dát v organizácii správcu sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru, - V organizácii správcu sa vypracuje a dodržiava politika zálohovania, ktorá definuje požiadavky organizácie správcu na zálohovanie vrátane doby uchovávaní, 	<p>V zmysle vyhlášky č. 179/2020 Z. z. správca musí prijať politiku zálohovania či interný riadiaci akt riadenia zmien.</p>

	<p>najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,</p> <ul style="list-style-type: none"> - tým, že prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povolené na princípe zásady najnižších privilégií, - prostredníctvom bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a 	<p>testovania záloh, ako aj opatrenia na ochranu záložných médií,</p> <ul style="list-style-type: none"> - Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykatel'ného priestoru. <p>Kategória II a Kategória III</p> <ul style="list-style-type: none"> - Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách, - Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči, - Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok, - Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú 	
--	---	--	--

	<p>vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,</p> <ul style="list-style-type: none"> - tým, že sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete, - tým, že spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov, - prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu, - udržiavaním zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave, 	<p>archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnnej pohromy,</p> <ul style="list-style-type: none"> - Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú. Za aktuálnosť prevádzkovej dokumentácie zodpovedajú správcovia jednotlivých informačných technológií verejnej správy, - Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien, - Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostných rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň, 	
--	--	--	--

	<ul style="list-style-type: none"> - použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou, - prostredníctvom blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje, - neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty, - prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete, - implementovaním systému detekcie prienikov alebo systému prevencie prienikov na 	<ul style="list-style-type: none"> - Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti, - V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien, - Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú na konkrétnych prvkoch informačných technológií verejnej správy, - Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti, - Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na 	
--	--	---	--

	<p>identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,</p> <ul style="list-style-type: none"> - prostredníctvom smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu, - prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete, - vykonávaním pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti. 	<p>prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.</p>	
--	---	--	--

<p>Hodnotenie zraniteľností a bezpečnostných aktualizácií</p>	<p>ZoKB ani vyhláška neobsahujú špecifická pre túto oblasť.</p>	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Nastavenie automatickej aktualizácie operačného systému a aplikácií. <p>Kategória II</p> <ul style="list-style-type: none"> - Zaviesť pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov, - Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou, - Vykonávanie hodnotenie zraniteľností najmenej raz ročne, - Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných 	<p>Hoci bola do ZoKB doplnená oblasť - hodnotenie zraniteľností a bezpečnostných aktualizácií, táto oblasť nie je upravená vo vyhláške č. 362/2018 Z. z. Predmetná vyhláška upravuje oblasť - technické zraniteľnosti informačných systémov a uvádza, akým spôsobom sa identifikujú.</p>
--	---	--	--

		<p>technológií verejnej správy v organizácii správcu,</p> <ul style="list-style-type: none"> - Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií, - Jednotlivé prvky informačných technológií verejnej správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií verejnej správy, - Pri identifikácii nových zraniteľností a bezpečnostných aktualizácií sa vychádza z konkrétnych zdrojov, - Výnimky z implementácie bezpečnostných aktualizácií sa schvaľujú a evidujú manažérom kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý určuje bezpečnostné opatrenia na ochranu pred zneužitím zraniteľnosti, na elimináciu ktorej je bezpečnostná aktualizácia vydaná, 	
--	--	---	--

		<ul style="list-style-type: none"> - Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií. - Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií verejnej správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou. - Po implementácii aktualizácie sa aktualizuje prvok informačných technológií verejnej správy verifikovaný, najmä jeho správna funkcionality. <p>Kategória III</p> <ul style="list-style-type: none"> - Preskúvanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov. 	
--	--	---	--

		<ul style="list-style-type: none"> - Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja. 	
Ochrana proti škodlivému kódu	ZoKB ani vyhláška neobsahujú špecifickú pre túto oblasť.	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácii škodlivým kódom, - V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru, - Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD; škodlivé emailové prílohy a odkazy; podozrivé a škodlivé webové stránky a odkazy; externú a internú sieťovú komunikáciu v organizácii správcu vrátane webových sídiel, prenos súborov z externých sietí, - Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí 	Hoci bola do ZoKB doplnená oblasť – ochrana proti škodlivému kódu, táto oblasť nie je upravená vo vyhláške č. 362/2018 Z. z.

		<p>kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.</p> <p>Kategória II</p> <ul style="list-style-type: none"> - Zavedenie ochrany informačných technológií verejnej správy pred škodlivým kódom v stanovenom rozsahu, - Zavedenie ochrany pred nevyžiadanou elektronickou poštou. <p>Kategória III</p> <ul style="list-style-type: none"> - Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu, - Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov, - Vypracovanie postupov obnovy a odstránenia infiltrácie škodlivým kódom na efektívne zvládanie infiltrácie škodlivým kódom. 	
--	--	---	--

<p>Sieťová a komunikačná bezpečnosť</p>	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - riadenie prístupov používateľov k sieťam a informačným systémom, - riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom, 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu, - Na sieťových zariadeniach sa implementujú najmenej konkrétne bezpečnostné opatrenia, - Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu. <p>Kategória II</p> <ul style="list-style-type: none"> - Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám, - Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením, - Správa počítačových sietí je riadená a kontrolovaná, - Pri prenose údajov prostredníctvom verejnej siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie 	<p>Vyhláška č. 362/2018 Z. z. preferuje používanie kryptografických prostriedkov a ich správu, kým bezpečnostné opatrenia v tejto oblasti podľa vyhlášky č. 179/2020 Z. z. sú koncipované širšie a zamerané na používanie firewallu či riadenie prenosu informácií.</p>
--	---	---	---

	<ul style="list-style-type: none"> - prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povolené na princípe zásady najnižších privilégií, - bezpečnostné opatrenia na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov, - sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete, - spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov, 	<p>dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb,</p> <ul style="list-style-type: none"> - Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment, - Sieťové služby, používatelia a jednotlivé prvky informačných technológií verejnej správy musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni, - Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia, - Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu, 	
--	--	---	--

	<ul style="list-style-type: none"> - servery dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu, - udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave, - použitie automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou, - blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje, - neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty, - systém monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj 	<ul style="list-style-type: none"> - Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov, - Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami, - Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu, - Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s tretou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii, 	
--	---	--	--

	<p>informácie o sieťových paketoch na hranici siete,</p> <ul style="list-style-type: none"> - implementovanie systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky, - smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu, vyžiadanie použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete, - vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného 	<ul style="list-style-type: none"> - Vzdialený prístup do vnútornej siete organizácie správcu musí podliehať autentifikácii a autorizácii. <p>Kategória III</p> <ul style="list-style-type: none"> - V organizácii správcu sa implementuje technológia detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete, - Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS, - Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom. 	
--	---	--	--

	zaručenia vrátane preukázania plnenia tejto povinnosti.		
Akvizícia, vývoj a údržba informačných sietí a informačných systémov	ZoKB ani vyhláška neobsahujú špecifickú pre túto oblasť.	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti. <p>Kategória II a Kategória III</p> <ul style="list-style-type: none"> - Pri vytváraní nových alebo úprave existujúcich informačných technológií verejnej správy sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť, - Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy 	Hoci bola do ZoKB doplnená oblasť – akvizícia, vývoj a údržba informačných sietí a informačných systémov, táto oblasť nie je upravená vo vyhláške č. 362/2018 Z. z.

		<p>organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov,</p> <ul style="list-style-type: none"> - Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou, - Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpoveďami, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov, - Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich 	
--	--	--	--

		<p>vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien,</p> <ul style="list-style-type: none"> - Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne, - Súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu, - Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre organizáciu správcu, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne 	
--	--	--	--

		<p>pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.</p>	
<p>Zaznamenávanie udalostí a monitorovanie</p>	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - Povinnosť využívať centrálny nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov, - Špecifikáciu minimálnych požiadaviek na vytváranie prevádzkových záznamov (logov), - Špecifikácia zabezpečenia prevádzkových záznamov (logov), - Určenie zodpovedného zamestnanca za monitorovanie. 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Zaznamenávanie úspešných a neúspešných autentifikačných udalostí. <p>Kategória II</p> <ul style="list-style-type: none"> - Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií verejnej správy. - Pre každý prvok informačných technológií verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované, 	<p>Vyhláška č. 179/2020 Z. z. upravuje udalosti a bezpečnostne relevantné udalosti. Tieto pojmy nie sú definované.</p>

		<ul style="list-style-type: none"> - Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej konkrétne udalosti, - Jednotlivé záznamy v log súboroch obsahujú najmenej konkrétne informácie o každej zaznamenanej udalosti, ak sú k dispozícii, - Záznamy udalostí sa uchovávajú najmenej šesť mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou, - Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií verejnej správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze, - Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident, - Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja. 	
--	--	--	--

		<p>Kategória III</p> <ul style="list-style-type: none"> - Správca vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií verejnej správy. - Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia. - Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach. - Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení. - Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni, 	
--	--	--	--

		<ul style="list-style-type: none"> - Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením, - Kapacita systémov uchovávajúcich záznamy musí byť adekvátne tak, že nedochádza k nežiaducemu prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania. 	
Fyzická bezpečnosť a bezpečnosť prostredia	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - umiestnenie siete a informačného systému v takom priestore, že sieť a informačný systém alebo aspoň ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor“), 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia. <p>Kategória II</p> <ul style="list-style-type: none"> - Umiestnenie informačných technológií verejnej správy v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými 	<p>Pri kategórii III. bezpečnostných opatrení odkazuje vyhláška č. 179/2020 Z. z. na opatrenia fyzickej bezpečnosti a bezpečnosti prostredia podľa vyhlášky č. 362/2018 Z. z.</p>

	<ul style="list-style-type: none"> - ochranu zabezpečeného priestoru fyzickými prostriedkami, najmä stenami, mechanickými zábrannými prostriedkami, technickými zabezpečovacími prostriedkami, napríklad zariadeniami elektrickej zabezpečovacej signalizácie, systémami na kontrolu vstupu, kamerovými systémami, - zaručenie, že sa v okolí zabezpečeného priestoru nevyskytujú zariadenia, ktoré môžu ohroziť sieť a informačný systém umiestnený v tomto zabezpečenom priestore, najmä kanalizácia, vodovod, horľavé alebo iné obdobné materiály, - vypracovanie, implementácie a kontroly dodržiavania pravidiel na prácu v zabezpečenom priestore, 	<p>dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa,</p> <ul style="list-style-type: none"> - Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami, - Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám, - Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj konkrétne uvedené pravidlá, - Prvky informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie. <p>Kategória III</p>	
--	---	--	--

	<ul style="list-style-type: none"> - zabezpečenie ochrany pred výpadkom zdroja elektrickej energie tých častí siete a informačného systému, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, že taký výpadok nenastane, - zaručenie, že existujú záložné kapacity siete a informačného systému, zabezpečujúce dostupnosť, funkčnosť alebo náhradu siete a informačného systému, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru, - zaručenie, že prevádzka, používanie a manažment siete a informačného systému je v súlade vnútornými predpismi a zmluvnými záväzkami, - politiky, ktorá zakazuje nechávanie fyzických 	<ul style="list-style-type: none"> - Podporná infraštruktúra informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora, - Pre informačné technológie verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií verejnej správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru, - Ďalšie opatrenia fyzickej bezpečnosti a bezpečnosti prostredia sa prijímajú podľa vyhlášky č. 362/2018 Z. z. 	
--	--	--	--

	<p>dokumentov bez dozoru a prikazuje uzamykanie počítača pred opustením pracoviska,</p> <ul style="list-style-type: none"> - organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania pravidiel v demonštratívne vymedzených oblastiach. 		
<p>Riešenie kybernetických bezpečnostných incidentov</p>	<p>Riešenie kybernetických incidentov musí obsahovať viaceré postupy a aktivity, vyhláška menuje hlavne:</p> <ul style="list-style-type: none"> - prípravu a vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, - monitorovanie a analýzu udalostí - zbieranie informácií, - vyhodnocovanie kybernetických bezpečnostných incidentov 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <ul style="list-style-type: none"> - V organizácii správcu sa určí kontaktné miesto a spôsob hlásenia kybernetických bezpečnostných incidentov podľa ZoITVS. <p>Kategória II</p> <ul style="list-style-type: none"> - Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov ZoITVS, bezpečnostne 	<p>ZoITVS upravuje len nahlasovanie kybernetických bezpečnostných incidentov. Vyhláška č. 179/2020 Z. z. upravuje aj hlásenie:</p> <ul style="list-style-type: none"> • bezpečnostne relevantných udalostí, • zraniteľností, • bezpečnostných slabých miest informačných

	<ul style="list-style-type: none"> - riešenie incidentov a zníženie ich následkov, - vyhodnocovanie spôsobov riešenia bezpečnostných incidentov. <p>Vyhláška ďalej bližšie špecifikuje ako sa zabezpečuje:</p> <ul style="list-style-type: none"> - Proces detekcie kybernetických bezpečnostných incidentov, - Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov, - Proces riešenia kybernetických bezpečnostných incidentov. 	<p>relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií verejnej správy, ktoré sú zistené pri ich používaní alebo správe,</p> <ul style="list-style-type: none"> - V organizácii správcu je na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov, - Interný riadiaci akt podľa písmena b) obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií verejnej správy, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií verejnej správy potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT, - S interným riadiacim aktom podľa písmena b), najmä povinnosťou ohlasovať 	<p>technológií verejnej správy.</p>
--	--	--	-------------------------------------

		<p>kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámia všetci používatelia informačných technológií verejnej správy vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií verejnej správy,</p> <ul style="list-style-type: none"> - Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách verejnej správy sa vytvára kontaktné miesto, - Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu, - Proces odborného posúdenia a analýzy oznámení realizuje Manažér kybernetickej bezpečnosti a informačnej bezpečnosti v spolupráci so správcami jednotlivých 	
--	--	---	--

		<p>komponentov a s vlastníkom/gestorom informačných technológií verejnej správy alebo príslušnou jednotkou CSIRT/CERT,</p> <ul style="list-style-type: none"> - Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov, - Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy, - Poznatky získané z procesu riešenia bezpečnostného incidentu, najmä z analýzy a spôsobu vyriešenia, sa premietajú do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov, ako aj na zlepšenie detekcie alebo spôsobu riešenia obdobných bezpečnostných incidentov. <p>Kategória III</p>	
--	--	---	--

		<ul style="list-style-type: none"> - Interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov okrem uvedených náležitostí podľa Kategórie II obsahuje aj ďalšie povinnosti a zodpovednosti v konkrétnych oblastiach. - Zamestnanci poverení riešením kybernetických bezpečnostných incidentov sú odborne spôsobilí, pravidelne školení a zastupiteľní. - V organizácii správcu sú vytvorené plány na riešenie kybernetických bezpečnostných incidentov. 	
Kryptografické opatrenia	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - Kryptografické prostriedky používajú dostatočne odolné kryptografické mechanizmy, pričom sa určia pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov, 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <p>Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS</p> <p>https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=181</p> <p>Kategória II a Kategória III</p>	

	<ul style="list-style-type: none"> - Systém správy kryptografických kľúčov a certifikátov je zabezpečený počas celého životného cyklu kryptografických kľúčov a certifikátov. Správa kryptografických kľúčov a certifikátov zahŕňa najmenej: <ul style="list-style-type: none"> • bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi, • generovanie pseudonáhodných čísel a kľúčov, zriadenie, distribúciu, vkladanie, zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zneplatnenie certifikátov, • umožnenie kontroly a auditu. 	<ul style="list-style-type: none"> - Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis, - Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie konkrétnych aktív, - Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje konkrétne požiadavky a princípy, - Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie, - Správca pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu. 	
--	---	--	--

<p>Kontinuita prevádzky</p>	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <ul style="list-style-type: none"> - Určenie požiadaviek na zabezpečenie kontinuity riadenia kybernetickej bezpečnosti pri vzniku kybernetického bezpečnostného incidentu, - Riadenie kontinuity procesov, ktoré pozostáva najmenej u konkrétnych aktivít a postupov. - Postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu. 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <p>Nevzťahujú sa žiadne bezpečnostné opatrenia.</p> <p>Kategória II a Kategória III</p> <ul style="list-style-type: none"> - Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú, - Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy, - Plán kontinuity prevádzky obsahuje konkrétne náležitosti, - Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne. 	
------------------------------------	--	---	--

<p>Audit, riadenie súladu a kontrolných činností</p>	<p>ZoKB obsahuje špecifikáciu tohto bezpečnostného opatrenia v § 29.</p> <p>Problematika auditovania a jeho právnej úpravy sa venujeme nižšie v časti dozor a dohľad.</p> <p>Relevantné špecifiká upravuje vyhláška č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora, ktorá rámcovo upravuje:</p> <ul style="list-style-type: none"> - Povinnosti audítora, - Náležitosti záverečnej správy. 	<p>Bezpečnostné opatrenia v tejto oblasti upravujú:</p> <p>Kategória I</p> <p>Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa vyhlášky Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.</p> <p>Kategória II a Kategória III</p> <ul style="list-style-type: none"> - Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy, - Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti, - Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad, 	<p>Vyhláška č. 179/2020 Z. z. v prípade oblasti auditu odkazuje na vyhlášku č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.</p>
---	--	--	---

		<ul style="list-style-type: none">- Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijímú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravujú sa tieto opatrenia tak, že bezpečnostné riziko znížené na prijateľnú úroveň.	
--	--	---	--

3.4.4. Identifikované problémy a návrhy riešení

ZoKB a ZoITVS podľa porovnávajúcich oblastí obsahujú viaceré rozdielne prístupy v oblasti bezpečnostných opatrení. V prvom rade je potrebné spomenúť, že **niektoré oblasti bezpečnostných opatrení v podzákonnom právnom predpise k ZoKB nie sú špecifikované, zatiaľ čo vyhláška ku ZoITVS ich obsahuje**. Konkrétne ide o oblasti:

- Akvizícia, vývoj a údržba informačných sietí a informačných systémov;
- Hodnotenie zraniteľností a bezpečnostných aktualizácií;
- Ochrana proti škodlivému kódu.

Máme za to, že pre dosiahnutie čo najväčšej jednoty a prepojitelnosti právnych rámcov by pokrývané oblasti mali byť totožné a špecifikované totožným spôsobom. Zároveň by bolo vhodné, **aby rámcové oblasti boli v ZoKB a ZoITVS pomenované rovnako**. Pre adresátov právnych noriem by to bolo prínosné aj z toho dôvodu, že ak ako referenčnú normu využívajú štandardy, bolo by to pre adresátov prehľadnejšie.

Vyššie analyzované oblasti bezpečnostných opatrení sú až na niektoré výnimky (napr. oblasť sieťovej komunikácie) upravené podobným spôsobom.

Rozlišujúcim aspektom pri realizácii konkrétnych bezpečnostných opatrení v zmysle ZoKB a ZoITVS a ich vyhlášok je **spôsob, akým sa určuje, ktoré oblasti bezpečnostných opatrení sa majú realizovať**. V prípade ZoKB a vyhlášky č. 362/2018 Z. z. prevádzkovateľ základnej služby realizuje bezpečnostné opatrenia na základe kategorizácie sietí a informačných systémov. V zmysle predmetnej vyhlášky sú definované 3 kategórie, konkrétne Kategória I, II a III. V závislosti od konkrétnej kategórie sa prevádzkovateľovi základnej služby **bud' len odporúča realizovať bezpečnostné opatrenia, alebo je to jeho povinnosť**.

Bezpečnostné opatrenie pre oblasť:	Kategória I	Kategória II	Kategória III
organizácie informačnej bezpečnosti	Odporúčané	Odporúčané	Povinné
riadenia aktív, hrozieb a rizík	Odporúčané	Povinné	Povinné
personálnej bezpečnosti	Odporúčané	Povinné	Povinné
riadenia dodávateľských služieb, akvizície,	Odporúčané	Povinné	Povinné

vývoja a údržby informačných systémov			
technických zraniteľností systémov a zariadení	Odporúčané	Povinné	Povinné
riadenia bezpečnosti sietí a informačných systémov	Odporúčané	Povinné	Povinné
riadenia prevádzky	Odporúčané	Povinné	Povinné
riadenia prístupov	Odporúčané	Povinné	Povinné
kryptografických opatrení	Odporúčané	Odporúčané	Povinné
riešenia kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
monitorovania, testovania bezpečnosti a bezpečnostných auditov	Odporúčané	Povinné	Povinné
fyzickej bezpečnosti a bezpečnosti prostredia	Odporúčané	Odporúčané	Povinné
riadenia kontinuity procesov	Odporúčané	Povinné	Povinné

V prípade **ZoITVS a vyhlášky č. 179/2020 Z. z. platí, že správca má povinnosť realizovať minimálne bezpečnostné opatrenia konkrétnej oblasti v závislosti od kategórie.** Predmetná vyhláška definuje tri kategórie minimálnych bezpečnostných opatrení a zároveň v rámci týchto kategórií uvádza výpočet správcov, na ktorých sa tieto bezpečnostné opatrenia vzťahujú. V tomto prípade vidieť iný prístup, aký sa aplikuje podľa ZoKB a vyhlášky č. 362/2018 Z. z., nakoľko **realizácia bezpečnostných opatrení konkrétnej oblasti nie je naviazaná na výsledok kategorizácie sietí a informačných systémov**, ale vo vyhláške č. 179/2020 Z. z. je pevne daný zoznam správcov v rámci konkrétnej kategórie.

Odišný prístup v otázke minimálnych bezpečnostných opatrení možno vidieť aj v **stupňovaní bezpečnostných opatrení v závislosti od konkrétnej kategórie v zmysle vyhlášky č. 179/2020 Z. z.** V prípade vyhlášky č. 362/2018 Z. z. takéto stupňovanie absentuje a subjekt musí prijať všetky definované bezpečnostné opatrenia, ak sú povinné.

Rizikom rozličnej metodiky realizácie minimálnych bezpečnostných opatrení je, že na ten istý subjekt sa možno budú vzťahovať minimálne bezpečnostné opatrenia podľa vyhlášky č. 362/2018 Z. z. napr. III kategórie, avšak podľa vyhlášky č. 179/2020 Z. z. sa daný subjekt vzťahujú napr. minimálne bezpečnostné opatrenia kategórie I.

S takouto situáciou bude súvisieť aj otázka, ktorá vyplýva z našej analýzy týkajúcej sa pôsobnosti, akým spôsobom správca v dvoch právnych postaveniach vyhodnotí takúto situáciu, a teda **ako relevantne bude vedieť porovnať, ktoré bezpečnostné opatrenia sú striktnejšie**. Ako bolo už uvedené, správca, ktorý je zároveň aj prevádzkovateľ základnej služby prijíma a realizuje bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe podľa ZoITVS a vyhlášky č. 179/2020 Z. z. ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje ZoKB.

V niektorých prípadoch bude porovnávanie jednoduché, napr. ak vyhláška č. 362/2018 Z. z. neupravuje oblasť, ktorá je definovaná vo vyhláške č. 179/2020 Z. z. (napr. akvizícia, vývoj a údržba informačných sietí a informačných systémov; hodnotenie zraniteľností a bezpečnostných aktualizácií; ochrana proti škodlivému kódu). Avšak v niektorých prípadoch bude určenie či je cieľom bezpečnostných opatrení dosiahnuť vyššiu úroveň bezpečnosti náročnejšie.

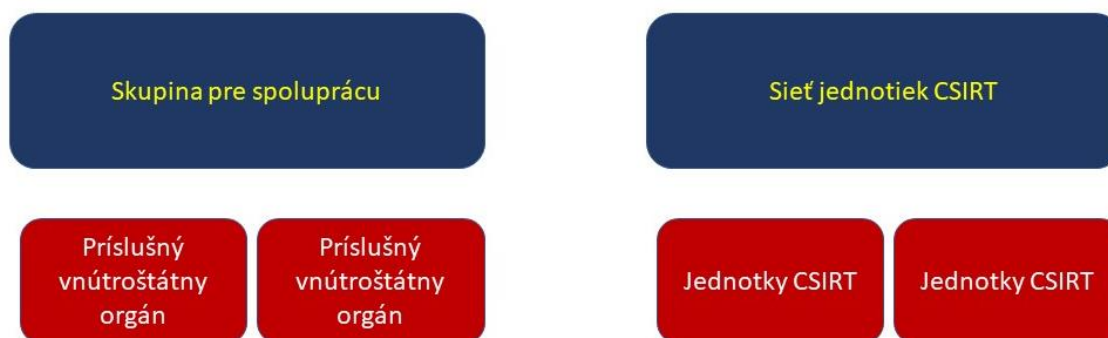
Bez toho, aby sa vyjasnil vzťah aplikácie ZoKB a ZoITVS v otázke osobnej pôsobnosti subjektov, ktorí sú správcami podľa ZoITVS a prevádzkovateľmi základnej služby podľa ZoKB, a bez toho, aby došlo k náprave nesúladu ZoKB so Smernicou NIS v otázke identifikácie prevádzkovateľov základnej služby v sektore verejná správa a podsektore informačné systémy verejnej správy, je formulácia akýchkoľvek riešení v tomto kontexte bezpredmetná.

3.5. Dozor a dohľad

3.5.1. Zákon o kybernetickej bezpečnosti

Dohľad a dozor podľa ZoKB zásadne ovplyvňuje Smernica NIS, ktorá určuje inštitucionálne mantinely a právomoci jednotlivých orgánov na úseku kybernetickej bezpečnosti. Smernica NIS vyžaduje zriadenie **príslušného vnútroštátneho orgánu** a jednu alebo viac **jednotiek CSIRT**.

Základnou úlohou príslušného vnútroštátneho orgánu je monitorovanie uplatňovania požiadaviek Smernice NIS.¹⁷⁷ Jednotky CSIRT na strane druhej zodpovedajú za riešenie rizík a incidentov.¹⁷⁸ Zároveň, členské štáty musia určiť tzv. jednotné kontaktné miesto, ktoré „*vykonáva styčnú úlohu, aby zabezpečilo cezhraničnú spoluprácu orgánov členských štátov s príslušnými orgánmi v iných členských štátoch, so skupinou pre spoluprácu uvedenou a sieťou jednotiek CSIRT.*“¹⁷⁹ Na úrovni spolupráce medzi členskými štátmi funguje skupina pre spoluprácu, ktorú tvoria zástupcovia členských štátov, Európskej komisie a agentúry ENISA. Základným cieľom skupiny pre spoluprácu je strategická spolupráca a výmena informácií.¹⁸⁰ Jednotky CSIRT operujú v rámci siete jednotiek CSIRT naprieč EÚ.¹⁸¹



Obrázok: Orgány dozoru a dohľadu podľa Smernice NIS.

ZoKB prirodzene špecifikuje národné vnútroštátne príslušné orgány a zriaďuje jednotky CSIRT. § 4 ZoKB definuje pôsobnosť orgánov verejnej moci na úseku kybernetickej bezpečnosti v Slovenskej republike.

Najdôležitejšiu úlohu plní **Národný bezpečnostný úrad SR**. Tento úrad plní aj úlohy jednotného kontaktného miesta.

Zákonná právna úprava ďalej definuje tzv. ústredné orgány a iné štátne orgány. **Ústrednými orgánmi** sú: Ministerstvo dopravy a výstavby Slovenskej republiky; Ministerstvo financií Slovenskej republiky; Ministerstvo hospodárstva Slovenskej republiky; Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky; Ministerstvo zdravotníctva Slovenskej republiky; Ministerstvo

¹⁷⁷ Smernica NIS, článok 8 ods. 1 a 2.

¹⁷⁸ Smernica NIS, článok 9 ods. 1.

¹⁷⁹ Smernica NIS, článok 8 ods. 4.

¹⁸⁰ Smernica NIS, článok 11 ods. 1.

¹⁸¹ Pozri bližšie Smernica NIS, článok 12.

životného prostredia Slovenskej republiky a Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.¹⁸² Ústredné orgány sú zodpovedné za aplikáciu primeraných bezpečnostných opatrení podľa ZoKB a majú plniť úlohy jednotiek CSIRT vo svojej pôsobnosti.

Iné štátne orgány sú vymedzené s odkazom na tzv. kompetenčný zákon. Plný výpočet iných štátnych orgánov zahŕňa ministerstvá, ktoré nie sú podľa ZoKB ústrednými orgánmi a ostatné ústredné orgány štátnej správy: Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu sieťových odvetví, Úrad vlády Slovenskej republiky; Protimonopolný úrad Slovenskej republiky; Štatistický úrad Slovenskej republiky; Úrad geodézie, kartografie a katastra Slovenskej republiky; Úrad jadrového dozoru Slovenskej republiky; Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky; Úrad pre verejné obstarávanie; Úrad priemyselného vlastníctva Slovenskej republiky; Správa štátnych hmotných rezerv Slovenskej republiky; Národný bezpečnostný úrad. Tieto orgány taktiež musia zabezpečiť plnenie opatrení na úseku kybernetickej bezpečnosti, ale na rozdiel od ústredných orgánov nemusia zriaďovať jednotky CSIRT.

3.5.1.1. NBÚ SR a dohľad

Úlohy a právomoci NBÚ SR podľa ZoKB sú primárne predmetom právnej úpravy v § 5, ale niektoré špecifické úlohy sa nachádzajú roztrúsené po celom právnom predpise ako napríklad blokovanie alebo auditovanie. Považujeme za vhodné, aby úlohy a právomoci NBÚ boli koncepčne upravené v osobitnej (samostatnej) časti zákona spolu s ich špecifikáciou.

Úloha pre MIRRI: Zákon o kybernetickej bezpečnosti

Koncepčne uchopiť úlohy a právomoci NBÚ pri revízii právneho rámca kybernetickej bezpečnosti.

Úlohy NBÚ možno rozdeliť do viacerých oblastí. Pre lepšie pochopenie uvádzame konkrétne úlohy a právomoci v tabuľke pre zjednodušenie daného prehľadu.

Rámcové úlohy		Špecifikácia
Koordinačné monitorovacie činnosti	a	<ul style="list-style-type: none">- riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti;- v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky

¹⁸² Bližšie pozri Príloha č. 1, ZoKB.

	<p>republiky a partnerov v rámci Európskej únie a Organizácie Severoatlantickej zmluvy;</p> <ul style="list-style-type: none"> - spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona; - systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike; - zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni; - zasiela včasné varovania;
Metodické a vzdelávacie činnosti	<ul style="list-style-type: none"> - určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore; - určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia; - vydáva znalostné štandardy a zverejňuje ich na svojom webovom sídle, a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia; - koordinuje výskum a vývoj; - vydávanie certifikačných postupov a schém;
Medzinárodná spolupráca	<ul style="list-style-type: none"> - je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy; - plní notifikačné a nahlásovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie Severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti; - zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT; - prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými

	organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom;
Organizačné a spravovacie úlohy	<ul style="list-style-type: none"> - spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti; - plní úlohy príslušného orgánu pre digitálne služby; - prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch; - plní úlohy kompetenčného a odvetvového centra podľa osobitného predpisu;
Registračné a certifikačné úlohy	<ul style="list-style-type: none"> - určuje a zaradzuje do zoznamov základné služby, digitálne služby, poskytovateľov digitálnych služieb a prevádzkovateľov základných služieb; - spravuje vyššie uvedené zoznamy a zoznam akreditovaných jednotiek CSIRT; - akredituje jednotky CSIRT okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT; - je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu; - zabezpečuje proces certifikácie kybernetickej bezpečnosti; - vedie a zverejňuje na svojom webovom sídle zoznam orgánov posudzovania zhody v systéme certifikácie kybernetickej bezpečnosti, zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti a zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti;
Kontrolné právomoci	<ul style="list-style-type: none"> - vykonáva kontrolu, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt; - vykonáva audit alebo požiada certifikovaného audítora kybernetickej bezpečnosti o vykonanie auditu u prevádzkovateľa základnej služby;
Vyšetrovacie právomoci	<ul style="list-style-type: none"> - posudzuje bezpečnostné riziká dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len

	„tretia strana“) pre kybernetickú bezpečnosť Slovenskej republiky a správu o tomto posúdení predkladá Bezpečnostnej rade Slovenskej republiky;
Ukladanie povinností a sankčné opatrenia	<ul style="list-style-type: none"> - rieši kybernetické bezpečnostné incidenty, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie; - rozhoduje o blokovaní škodlivého obsahu alebo škodlivej aktivity, ktorá smeruje do kybernetického priestoru Slovenskej republiky alebo z kybernetického priestoru Slovenskej republiky (ďalej len „blokovanie“) a zabezpečuje vykonanie tohto rozhodnutia alebo vykonáva blokovanie na základe žiadosti;
Oznamovacie povinnosti	<ul style="list-style-type: none"> - vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi; - predkladá príslušnému osobitnému kontrolnému výboru Národnej rady Slovenskej republiky každoročne správu o dodržiavaní noriem týkajúcich sa ochrany telekomunikačného tajomstva a osobných údajov občanov Slovenskej republiky.

NBÚ ako príslušný orgán pre oblasť kybernetickej bezpečnosti disponuje pomerne silnými opatreniami a právomocami. Povinnosti dotýkajúce sa kontroly, vyšetrovania a ukladania sankčných opatrení patria k tým najinvazívnejším z pohľadu prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb. Z tohto pohľadu by si konkrétne **vyšetrovacie právomoci** zaslúžili bližšiu špecifikáciu. Ako príklad možno uviesť oblasť ochrany osobných údajov, kde v GDPR¹⁸³ a aj slovenskom zákone o ochrane osobných údajov¹⁸⁴ nájdeme pomerne presne nastavené opatrenia a právomoci pri výkone vyšetrovania a kontroly. ZoKB síce odkazuje na všeobecný zákon o kontrole v štátnej správe,¹⁸⁵ otázkou ale je, či daný zákon postačuje požiadavkám a podmienkam pre výkon kontroly v oblasti kybernetickej bezpečnosti. Špecifickjšiu úpravu v § 29 ZoKB obsahuje **audit** kybernetickej bezpečnosti, i keď daná právna úprava sa týka primárne otázok ako kto môže audit vykonať, za akých podmienok a čo je jeho cieľom. Je potrebné ale upozorniť na § 29 ods. 6, v zmysle ktorého: „*Úrad môže kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u*

¹⁸³ GDPR, článok článok 58.

¹⁸⁴ Zákon o ochrane osobných údajov, § 81 ods. 2 a 3.

¹⁸⁵ Zákon Národnej rady Slovenskej republiky č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.

prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.“ V prípade auditovania subjektov štátom je vhodné, aby právna úprava upravovala presný proces vykonania auditu. V súvisiacej vyhláške NBÚ 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora sa napríklad nenachádzajú procesné práva auditovanej osoby, ak audit vykonáva štát.

Úloha pre MIRRI: Zákon o kybernetickej bezpečnosti

Koncepčne uchopiť výkon vyšetrovania auditovania pri revízii právneho rámca kybernetickej bezpečnosti.

Osobitne problematickým inštitútom je **blokovanie webových stránok** v zmysle § 27b a § 27c ZoKB. V zmysle danej právnej úpravy môže NBÚ vydať rozhodnutie o blokovaní webstránky, na ktorej sa nachádza škodlivý obsah. Škodlivý obsah je legálne definovaný ako „programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov alebo citlivých údajov, závažné dezinformácie a iné formy hybridných hrozieb.“¹⁸⁶ Pri procesnom postupe viaceré ustanovenia odkazujú na tzv. Pravidlá blokovania, ktoré ani na záver júna neboli publikované v právnej forme. NBÚ môže z vlastnej iniciatívy rozhodnúť o blokovaní iba s platnosťou do 30. júna 2022. Na blokovania za podnet iného orgánu sa daný limit nevzťahuje.¹⁸⁷ Zaujímavosťou je, že v prípade blokovania na žiadosť iného subjektu: „*náklady spojené s výkonom blokovania na základe žiadosti žiadateľa a zodpovednosť za škodu spôsobenú blokovaním znáša žiadateľ.*“ Ide o pomerne jedinečný prenos zodpovednosti pri výkone štátnej moci v slovenskom právnom poriadku na nahlasovateľa.

Samotný mechanizmus blokovania webstránok bol podrobený odbornej kritike.¹⁸⁸ Aj judikatúra Európskeho súdu pre ľudské práva a Súdneho dvora EÚ¹⁸⁹ formuluje jasné požiadavky na mechanizmus blokovania webstránok. V skratke, mechanizmus blokovania musí byť kompletne upravený v zákone. Nestačí, že časť mechanizmu bude súčasťou podzákonného právneho aktu alebo stáť úplne mimo právneho rámca v podobe usmernenia. Súčasný prístup je preto ústavne neudržateľný. Navyše, v zmysle uvedenej judikatúry musí blokovanie disponovať penzom záruk proti zneužitú. Menovať možno predovšetkým 4:

¹⁸⁶ ZoKB, § 27b ods. 3.

¹⁸⁷ Pozri ZoKB, § 27c ods. 9.

¹⁸⁸ Pozri napríklad HUSOVEC, M. Súčasný blokovanie dezinformačných stránok je ústavne problematické. Čo s tým? Denník N. Dostupné na: <https://dennikn.sk/2818631/sucasne-blokovanie-dezinformacnych-stranok-je-ustavne-problematicke-co-s-tym/?ref=list>.

¹⁸⁹ Pozri rozhodnutia Európskeho súdu pre ľudské práva vo veci Kharitonov proti Rusku, sťažnosť č. 10795/14; Bulgakov proti Rusku, sťažnosť č. 20159/15; Engels proti Rusku, sťažnosť č. 61919/16; OOO Flavus a ostatní proti Rusku, sťažnosť č. 12468/15. K hlbšej analýze jednotlivých záruk blokovania pozri HUSOVEC, M (Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement. Dostupné na SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784149.

- 1) Posúdenie vplyvu v legislatívnom procese – akýkoľvek invazívnejší zásah do práv a slobôd musí prejsť prísny posúdením vplyvu ešte pred prijatím právnej úpravy. V slovenskej právnej realite je ale posúdenie vplyvu častokrát iba formálne naplnenie tabuľky bez tvrdších dát;
- 2) Nezávislý dohľad – blokovanie musí byť predmetom prieskumu *ex-ante*, nie len *ex-post*. To znamená, že na mechanizmus musí dohliadať na to určený orgán (vo veľkej väčšine prípadov súd), ktorý musí mať zároveň právomoci rozhodnutie o blokovaní zvrátiť.
- 3) Transparentnosť – rozhodnutia o blokovaní by mali byť transparentne dostupné verejnosti. Zároveň, ak užívateľ príde na webstránku, ktorá je blokovaná, mal by mať nárok vedieť, prečo sa nemôže dostať k informáciám, ktoré vyhľadáva.
- 4) Spravodlivý proces – mechanizmus blokovania musí spĺňať atribúty spravodlivého procesu. To znamená, že iba v najviac ojedinelých prípadoch by malo dochádzať k blokovaní bez predošlého upozornenia prevádzkovateľa webu a lehoty na odstránenie nezákonného obsahu. Zároveň by mal prevádzkovateľ disponovať možnosťou sa voči rozhodnutiu brániť a to nielen súdnou cestou. Proces blokovania musí rešpektovať „rovnosť zbraní.“

Viacere z vyššie uvedených požiadaviek mechanizmus blokovania nespĺňa. Azda najvýraznejšie chýbajú záruky obrany proti rozhodnutiu (okrem napadnutia na súde) a transparentnosti. Nezávislý dohľad nad rozhodnutiami NBÚ zabezpečený nie je a privítali by sme rolu nezávislých súdov pri takomto procese.

Úloha pre MIRRI: Zákon o kybernetickej bezpečnosti

Koncepčne uchopiť blokovanie webových stránok a pri legislatívnom procese vyzývať na rešpektovanie judikatúry Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie.

3.5.1.2. Jednotky CSIRT a ich úlohy

Okrem príslušného orgánu v rámci Slovenskej republiky pôsobia aj jednotky CSIRT. Konkrétne sú zriadené:

- Národná jednotka CSIRT podľa § 6 ZoKB;
- Vládna jednotka CSIRT v pôsobnosti Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky pre podsektor informačné systémy verejnej správy podľa § 11 ZoKB; a
- Akreditované jednotky CSIRT, ktorými musia disponovať ústredné orgány.

Činnosť jednotiek CSIRT je rámcovaná kybernetickými bezpečnostnými incidentami. Jednotky CSIRT primárne zodpovedajú za riešenie kybernetických bezpečnostných incidentov a vykonávajú

preventívne služby a reaktívne služby.¹⁹⁰ Preventívne úlohy sú vymedzené v ZoKB taxatívne, reaktívne demonštratívnym spôsobom. Konkrétne ide o tieto úlohy:

Preventívne úlohy zamerané na prevenciu kybernetických bezpečnostných incidentov	vytváranie bezpečnostného povedomia
	výcvik
	spolupráca s ostatnými jednotkami CSIRT
	monitorovanie a evidencia kybernetických bezpečnostných incidentov
	pripojenie na jednotný informačný systém kybernetickej bezpečnosti
	poskytovanie informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti
	prijímanie a zasielanie včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti
Reaktívne úlohy zamerané na prevenciu kybernetických bezpečnostných incidentov	výstraha a varovanie
	detekcia kybernetických bezpečnostných incidentov
	analýza kybernetických bezpečnostných incidentov
	odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov
	asistencia pri riešení kybernetického bezpečnostného incidentu na mieste
	reakcia na kybernetický bezpečnostný incident
	podpora reakcií na kybernetické bezpečnostné incidenty
	koordinácia reakcií na kybernetické bezpečnostné incidenty
	návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov

¹⁹⁰ ZoKB, § 15.

V zmysle Smernice NIS, musia jednotky CSIRT disponovať najmä tromi kategóriami oprávnení a to konkrétne:

Oblasť	Úloha
Kybernetické bezpečnostné incidenty	<ul style="list-style-type: none"> ▪ monitorovanie incidentov na vnútroštátnej úrovni; ▪ vydávanie včasného varovania, upozornení, oznamovanie a šírenie informácií o rizikách a incidentoch príslušným zainteresovaným stranám; ▪ reagovanie na incidenty; ▪ zabezpečovanie dynamickej analýzy rizík a incidentov a získavanie informácií o situácii; ▪ účasť na činnosti siete jednotiek CSIRT.
Spolupráca	Jednotky CSIRT nadviažu spoluprácu so súkromným sektorom.
Štandardizácia	<p>V záujme uľahčenia spolupráce jednotky CSIRT podporujú prijímanie a využívanie spoločnej alebo normalizovanej praxe v oblasti:</p> <ul style="list-style-type: none"> ▪ postupov na riešenie incidentov a rizík; ▪ systémov klasifikácie incidentov, rizík a informácií.

Ak porovnáme úlohy jednotiek CSIRT v ZoKB a Prílohe č. I Smernice NIS, máme za to, že požiadavky na úlohy týkajúce sa kybernetických bezpečnostných incidentov sú splnené, dokonca nadštandardne. Štandardizačné úlohy a ich zákonná úprava je striedma, vyčítať to možno iba z reaktívnej úlohy v podobe „*návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.*“ Je však možné, že zákonodarca skôr danou úlohou zamýšľal konkrétny reaktívny postup pri riešení konkrétneho kybernetického bezpečnostného incidentu. Z tohto dôvodu považujeme za vhodné, aby priamo ZoKB upravoval štandardizačné úlohy jednotiek CSIRT explicitnejšie spôsobom. Úlohy v oblasti spolupráce so súkromným sektorom v legislatívnej úprave absentujú absolútne.

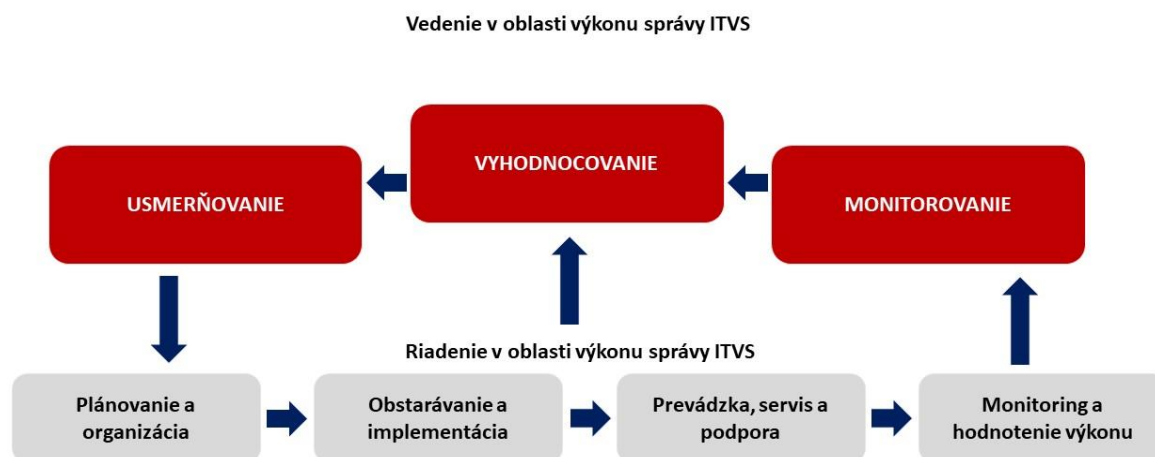
Úloha pre MIRRI: Zákon o kybernetickej bezpečnosti

Zabezpečiť pri revízii právneho rámca kybernetickej bezpečnosti precíznejšiu transpozíciu úloh jednotiek CSIRT v oblasti štandardizácie a spolupráce so súkromným sektorom.

3.5.2. Zákon o informačných technológiách vo verejnej správe

ZoITVS je pri legislatívnom vymedzení dozoru a dohľadu oproti ZoKB stručnejší. Úlohy v oblasti dohľadu nad dodržiavaním povinností podľa ZoITVS sú priradené tzv. orgánu vedenia, ktorým je MIRRI.¹⁹¹ Vedenie (po anglicky *governance*) v danej oblasti znamená: „činnosť orgánu vedenia v rozsahu jeho pôsobnosti podľa tohto zákona, ktorej účelom je riadny a efektívny výkon riadenia v správe informačných technológií verejnej správy podľa zákona a dosiahnutie cieľov informatizácie a rozvoja informačných technológií verejnej správy, ktoré vyplývajú z národnej koncepcie a ďalších koncepčných a strategických dokumentov s celoštátnou pôsobnosťou.“¹⁹² O úroveň nižšie pôsobia orgány riadenia, ktoré taxatívne vymenúva ZoITVS v § 5 ods. 2. Orgány riadenia majú v správe informačné technológie verejnej správy, pričom ale zodpovednosť za vytváranie, správu a rozvoj informačnej technológie verejnej správy zodpovedá správca.¹⁹³ Samotný pojem správca je definovaný v § 2 ods. 5 ZoITVS: „Správcom na účely tohto zákona je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe tohto zákona. Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely tohto zákona ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby; ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy.“

V zmysle dôvodovej správy možno vzťahy vedenia a riadenia graficky znázorniť na obrázku nižšie.



Obrázok: Vedenie a riadenie v oblasti výkonu správy informačných technológií verejnej správy.

¹⁹¹ ZoITVS, § 5 ods. 1 písm. a).

¹⁹² ZoITVS, § 7.

¹⁹³ ZoITVS, § 11 ods. 2.

Kľúčové úlohy dozoru na úseku IT vo verejnej správe vykonáva orgán vedenia (MIRRI). Tieto úlohy sú predmetom ustanovení v § 8 a 9 ZoITVS. Podobne ako pri ZoKB, úlohy možno rozdeliť do viacerých oblastí, ktoré uvádzame v tabuľke.

Rámcové úlohy	Špecifikácia
Usmerňovanie a koordinovanie správy IT vo verejnej správe	<ul style="list-style-type: none"> - monitorovanie výkonu riadenia v správe informačných technológií verejnej správy na účely sledovania aktuálneho stavu v správe informačných technológií verejnej správy a ich vývoji a sledovanie spôsobov a postupov pri vykonávaní tejto správy, - určovanie koncepcie štátnej politiky jednotného digitálneho trhu, - koordinácia budovania informačných technológií verejnej správy vrátane ich uvádzania do prevádzky a rozhodovanie o využívaní finančných zdrojov na ich budovanie a rozvoj v rozsahu ustanovenom zákonom, - určovanie centrálnej architektúry budovania a rozvoja informačných technológií verejnej správy (ďalej len „centrálna architektúra“) a referenčnej architektúry budovania a rozvoja informačných technológií verejnej správy (ďalej len „referenčná architektúra“), - určovanie gestora základného číselníka okrem základného číselníka životných situácií a základného číselníka úsekov verejnej správy a agend verejnej správy, riadenie, koordinácia a usmerňovanie vydávania, zverejňovania a spravovania základných číselníkov a rozhodovania sporov medzi orgánmi riadenia týkajúce sa vytvárania, zverejňovania alebo správy základných číselníkov, - riadenie, koordinovanie a usmerňovanie činnosti integrovaných obslužných miest.
Vyhodnocovanie	<ul style="list-style-type: none"> - vyhodnocovanie informácií získaných z monitorovania, kontroly a z iných podnetov na účely identifikácie rizík a nedostatkov v správe informačných technológií verejnej správy.
Monitorovanie	<ul style="list-style-type: none"> - vydávanie metodických usmernení, usmerňovanie a koordinácia orgánov riadenia na účely jednotného spôsobu

	<p>výkonu riadenia v správe informačných technológií verejnej správy a centrálneho riadenia informatizácie spoločnosti,</p> <ul style="list-style-type: none"> - určovanie kľúčové indikátory monitorovania pre jednotlivé úseky riadenia na účely monitorovania výkonu riadenia v správe informačných technológií verejnej správy.
Tvorba strategických dokumentov	<ul style="list-style-type: none"> - vypracúvanie, aktualizovanie a predkladanie národnej koncepcie vláde Slovenskej republiky , - usmerňovanie tvorby koncepcií rozvoja informačných technológií verejnej správy orgánom riadenia.
Notifikačné povinnosti a organizačné povinnosti	<ul style="list-style-type: none"> - informovanie vlády o stave a rozvoji informačných technológií verejnej správy, - zverejňovanie rozhodnutí na ústrednom portáli, iných dokumentov a informácii týkajúcich sa informačných technológií verejnej správy a informatizácie verejnej správy, - vydávanie a spravovanie zoznamu základných číselníkov, základného číselníka životných situácií a základného číselníka úsekov verejnej správy a agend verejnej správy, - zabezpečovanie poskytovania služieb v oblasti informačných technológií verejnej správy pre orgán riadenia po dohode s ním, ak je to potrebné na účely dosahovania cieľov v správe informačných technológií verejnej správy podľa § 7 alebo pre potreby verejného obstarávateľa na účely spolupráce podľa osobitného predpisu; tieto služby môže zabezpečovať aj prostredníctvom právnickej osoby vo svojej zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti.
Štandardizácia	<ul style="list-style-type: none"> - koordinácia tvorby všeobecne záväzných právnych predpisov v oblasti informačných technológií verejnej správy, - konzultácie návrhov dokumentov, ktoré majú dosah na informačné technológie verejnej správy, s osobami dotknutými týmito dokumentmi, - vydávanie štandardov a výkladových stanovísk, - môže pre orgán riadenia zabezpečiť prístup k normám a referenčným rámcom, ktoré sú využívané v správe informačných technológií verejnej správy, ak nie sú bežne dostupné; ak ide o technické normy, ktorých poskytovanie upravuje osobitný predpis,7) prístup sa zabezpečuje

	<p>prostredníctvom Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky spôsobom a za podmienok podľa tohto osobitného predpisu,</p> <ul style="list-style-type: none"> - zabezpečovanie organizačných predpokladov na zapojenie zástupcov odbornej verejnosti do tvorby pravidiel v správe informačných technológií verejnej správy a ich účasť na ich pripomienkovaní.
Vnútroštátna spolupráca	<ul style="list-style-type: none"> - zabezpečovanie zdieľanie informácií a skúseností medzi orgánmi riadenia prostredníctvom centrálného metainformačného systému verejnej správy, - poskytovanie v centrálnom metainformačnom systéme verejnej správy komunikačnú platformu pre zadávanie podnetov k správe informačných technológií verejnej správy, službám verejnej správy, službám vo verejnom záujme a k verejným službám, vyhodnocuje tieto podnety a ich inovačný potenciál a vedie mapu kritických miest integrovanej infraštruktúry a zverejňovanie datasetu otvorených dát o podnetoch zadaných spôsobom vrátane spôsobu riešenia a časovej odozvy.
Kontrola a sankcionovanie	<ul style="list-style-type: none"> - kontrolovanie dodržiavanie povinností orgánmi riadenia, - prijímanie opatrenia na nápravu zistených nedostatkov a ukladá pokuty za porušenie povinností ustanovených ZoITVS.

Ak porovnáme úlohy orgánu vedenia podľa ZoITVS a NBÚ podľa ZoKB, prirodzenie sa dané úlohy dopĺňajú, ale nie sú totožné. Dôvodom je odlišná filozofická koncepcia ZoKB a jej transpozícia zo Smernice NIS v porovnaní so špecifickou národnou právnou úpravou, ktorú predstavuje ZoITVS. Orgán vedenia napríklad nedisponuje právomocou blokovať webstránky so škodlivým obsahom alebo možnosťou vykonať audit na úrovni ZoKB.

V oblasti kontroly je podobne ako ZoKB potrebné doplniť, že právna úprava konkrétne procesné postupy rieši iba odkazom na všeobecný právny predpis o kontrole v štátnej správe.¹⁹⁴ Zároveň, „...vykonávaním niektorých činností pri kontrole dodržiavania štandardov, okrem kontroly dodržiavania podmienok týkajúcich sa bezpečnosti, môže orgán vedenia poveriť inú osobu, pričom rozsah týchto činností orgán vedenia určí v poverení v rozsahu svojej pôsobnosti.“¹⁹⁵ Podobne ako pri ZoKB by bolo vhodné zakotviť osobitné pravidlá pre kontrolu a právomoci kontrujujúceho orgánu po vzore iných legislatív, nakoľko všeobecná právna úprava kontroly v štátnej správe nemusí nevyhnutne reflektovať

¹⁹⁴ ZoITVS, § 9 ods. 2.

¹⁹⁵ ZoITVS, § 9 ods. 3.

potreby kontroly informačných systémov a kybernetickej bezpečnosti. Zároveň, ak má byť ambíciou ZoITVS čo najviac reflektovať ZoKB, úlohy a právomoci orgánu vedenia by mali byť čo najviac zosúladené s úlohami NBÚ podľa ZoKB.

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe
Zabezpečiť pri revízii právneho rámca kvalitnejšiu reflexiu úloh a právomoci orgánu vedenia a upraviť špecifický postup pri výkone kontroly.

Osobitnou otázkou je možnosť auditovania podľa ZoITVS. Tá je totiž upravená iným spôsobom ako v ZoKB, kde je explicitne ustanovená v jeho zákonomnom znení ako odlišný postup od kontroly. Audity sú v ZoITVS upravené dvojakým spôsobom a to ako (i) možno vykonať audit zo strany orgánu vedenia a (ii) povinnosť správcov zabezpečiť vykonanie bezpečnostného auditu. Orgán vedenia má právomoc v zmysle § 23 ods. 4 písm. d) ZoITVS **vykonať bezpečnostný audit**: *„Orgán vedenia vo vzťahu k informačným technológiám verejnej správy môže na žiadosť orgánu riadenia za tento orgán riadenia vykonať bezpečnostný audit alebo preň vykonať hodnotenie zraniteľnosti.“* Orgán vedenia teda môže vykonať bezpečnostný audit len vo vzťahu k informačným technológiám verejnej správy za podmienky, že ho o to požiada orgán riadenia. Napríklad, ak obec alebo vyšší územný celok sama požiada o vykonanie bezpečnostného auditu orgán vedenia, ktorým je MIRRI. V rámci bezpečnostného auditu v zmysle § 23 ods. 4 písm. d) ZoITVS môže MIRRI skúmať či boli splnené požiadavky v zmysle ZoITVS a vyhlášky č. 179/2020 Z. z. V zmysle tohto ustanovenia je vylúčené, aby MIRRI *ex offa* samo od seba začalo bezpečnostný audit. Zároveň je však nevyhnutné dodať, že pre bezpečnostný audit v zmysle § 23 ods. 4 písm. d) ZoITVS nie sú v ZoITVS a ani vo vyhláške č. 179/2020 Z. z. upravené žiadne podmienky, čo sa týka rozsahu bezpečnostného auditu, osoby, ktorá má právomoc vykonávať audit, otázok zaujatosti osoby vykonávajúcej audit, právomoci osoby pri kontrole, povinnosť mlčanlivosti či podrobné otázky týkajúce sa ukladania pokút.

Druhým súvisiacim inštitútom je povinnosť správcu zabezpečiť vykonanie bezpečnostného auditu. V zmysle § 21 ods. 3 písm. b) bod 6 ZoITVS je správca povinný v rámci zabezpečenia prevádzky informačného systému verejnej správy zabezpečiť vykonanie bezpečnostného auditu informačného systému verejnej správy v pravidelných intervaloch. Bližšie je táto povinnosť špecifikovaná vo Vyhláške č. 179/2020 Z. z. V zmysle prílohy č. 2 vyhlášky č. 179/2020 Z. z. (P. Audit a kontrolné činnosti) sa na zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti vzťahuje Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora (ďalej len „vyhláška č. 436/2019 Z. z.“). **Považujeme za potrebné zvýrazniť, že bezpečnostný audit v zmysle § 23 ods. 4 písm. d) ZoITVS (audit zo strany orgánu vedenia vid' body 1.3 - 1.5 tejto analýzy) nie je bezpečnostným auditom v zmysle § 21 ods. 3 písm. b) bod 6 ZoITVS a vyhlášky č. 179/2020 Z. z.**

Riešením je výslovné **zakotvenie možnosti MIRRI ako orgánu vedenia začať kontrolu alebo audit o kybernetickej bezpečnosti do ZoITVS**. V prípade zakotvenia auditu je nanajvýš

žiadané, aby zároveň bola koncipovaná vyhláška, ktorá špecifikuje konkrétne parametre auditu po vzore vyhlášky č. 436/2019 Z. z. Nevyhnutnosťou by malo byť prijatie samostatnej vyhlášky, ktorá bude upravovať audit podľa ZoITVS za predpokladu, že bude zakotvenie možnosti začať audit o kybernetickej bezpečnosti zo strany MIRRI. Audit by sa však mal vzťahovať iba na správcov, ktorí nemajú postavenie prevádzkovateľa základnej služby podľa ZoKB. V takom prípade by sa vytvorila (prakticky) totožná povinnosť, akú už dnes majú. Preto je potrebné vykonať právnu úpravu ZoITVS a vyhlášky č. 179/2020 Z. z, v zmysle ktorej by správcovia boli povinní zabezpečiť výkon bezpečnostného auditu v zmysle ZoITVS a príslušnej novej vyhlášky o audite. V prípade správcov, ktorí sú zároveň aj prevádzkovateľmi základných služieb podľa ZoKB by sa postupovalo v zmysle ZoKB a vyhlášky č. 436/2019 Z. z. Navrhovaná zmena je opodstatnená, nakoľko v súčasnosti sa pri bezpečnostnom audite podľa vyhlášky č. 436/2019 Z. z. overuje či správcovia plnia povinnosti podľa ZoKB a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa ZoKB. **Je potrebné podotknúť, že nie všetci správcovia sú zároveň aj prevádzkovateľmi základnej služby podľa ZoKB, a teda nie je účelné a vhodné, aby sa v prípade správcov, na ktorých sa vzťahuje len ZoITVS, overovalo splnenie bezpečnostných požiadaviek v zmysle ZoKB.**

Úloha pre MIRRI: Zákon o informačných technológiách vo verejnej správe

V prípade potreby analyzovať potrebu zavedenia auditovania ex offa zo strany orgánu vedenia a prispôbiť týmto záverom právnu úpravu v ZoITVS.

3.5.3. Identifikované problémy a návrhy riešení

Na problematické ustanovenia či už ZoKB alebo ZoITVS v kontexte dozoru a dohľadu sme upozornili vyššie. V prvom rade máme za to, že vyšetrovacie právomoci NBÚ a orgánu vedenia by mali byť upravené koncepčnejšie a nie iba odkazom na všeobecnú právnu úpravu kontroly v štátnej správe. Oblasť kybernetickej bezpečnosti je natoľko osobitá, že podľa nášho názoru vyžaduje osobitnú úpravu kontroly a právomoci orgánov pri ich výkone po vzore regulácii na úseku ochrany osobných údajov. Ak porovnáme úlohy orgánu vedenia podľa ZoITVS a NBÚ podľa ZoKB, prirodzené sa dané úlohy dopĺňajú, ale nie sú totožné. Dôvodom je odlišná filozofická koncepcia ZoKB a jej transpozícia zo Smernice NIS v porovnaní so špecifickou národnou právnou úpravou, ktorú predstavuje ZoKB. Orgán vedenia napríklad nedisponuje právomocou blokovať webstránky so škodlivým obsahom alebo možnosťou vykonať audit na úrovni ZoKB. Ak by orgán vedenia takouto právomocou disponoval, nebolo by to účelné, nakoľko blokovanie v zmysle ZoKB nie je obmedzené na prevádzkovateľov základných služieb resp. poskytovateľov digitálnych služieb.

Osobitne sme rozobrali problematiku blokovania webových stránok, ktoré je v súčasnom nastavení zjavne protiústavné a nerešpektuje konštantnú judikatúru Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva. Daný mechanizmus je potrebné zásadne revidovať a preformulovať. Zároveň, problematika auditovania by sa taktiež zaslúžila revíziu v ZoKB minimálne

z pohľadu procesného postupu, ak audit vedie štátny orgán. V ZoITVS sa prikláňame k možnosti, aby auditovať mohol aj orgán vedenia ex offa, dnes to môže iba na požiadanie konkrétneho subjektu. Za problematické považujeme aj nedostatočnú transpozíciu úloh jednotiek CSIRT v zmysle prílohy 1 Smernice NIS, kde slovenský zákonodarca niektoré úlohy opomenul zákonne upraviť.

3.6. Sankcie

3.6.1. Zákon o kybernetickej bezpečnosti

ZoKB upravuje sankcie, ktorými disponuje NBÚ vo viacerých úrovniach. V prvom rade je nevyhnutné spomenúť iné sankcie, ako sú správne pokuty. NBÚ môže:

- Rozhodnúť o obmedzení používania produktu, procesu, služby alebo tretej strany podľa § 27a; alebo
- Blokovat' škodlivý obsah podľa §§ 27b a 27c.

Z hľadiska ukladania pokút rozlišuje ZoKB medzi priestupkami, ktorých sa môže dopustiť len fyzická osoba a správnymi deliktami, ktorých sa môže dopustiť aj právnická osoba.

Priestupky sú upravené v § 30 ZoKB a NBÚ môže uložiť pokutu od 100 eur do 5 000 eur tomu, kto:

- poruší povinnosť uvedenú v § 12 ods. 1 týkajúcu sa mlčanlivosti a ochrany osobných údajov;
- poskytla nepravdivé údaje v oznámení na zaradenie základnej služby alebo prevádzkovateľa základnej služby podľa § 17 ods. 4;
- poruší niektorú z povinností prevádzkovateľa základnej služby podľa § 19 ods. 1 až 4, 6 alebo ods. 7;
- neprijme bezpečnostnú dokumentáciu podľa § 20 ods. 6; alebo
- nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby.

Na ukladanie pokút sa vzťahuje všeobecná právna úprava priestupkov. Zodpovednosť za priestupok tým zaniká, ak od jeho spáchania uplynuli dva roky; nemožno ho tiež prejednať, prípadne uloženú sankciu alebo jej zvyšok vykonať, ak sa na priestupok vzťahuje amnestia.¹⁹⁶

Pokuty za spáchanie správnych deliktov možno uložiť v rôznej výške, rôznym subjektom a za rôzne skutkové podstaty. Vzhľadom na variabilitu správnych deliktov ich uvádzame v tabuľke nižšie.

Výška pokuty	Subjekt	Porušenie
Od 300 € do 30 000 €	Prevádzkovateľovi základnej služby	<ul style="list-style-type: none">▪ Porušenie povinností prevádzkovateľov základných služieb podľa § 19 ods. 2 až 4 a 7,▪ Porušenie povinnosti udržiavať bezpečnostnú dokumentáciu aktuálnu a

¹⁹⁶ Zákon o priestupkoch, § 20 ods. 1.

		zodpovedajúcu reálnemu stavu podľa § 20 ods. 6.
Od 300 € do výšky 1 % celkového ročného obratu¹⁹⁷ za predchádzajúci účtovný rok, najviac však 300 000 €	Prevádzkovateľovi základnej služby	<ul style="list-style-type: none"> ▪ Neoznámenie prekročenia kritérií prevádzkovateľa základnej služby, ▪ Porušenie povinností podľa § 19 ods. 1 a ods. 6 ▪ Neprijatie bezpečnostnej dokumentácie podľa § 20 ods. 6, ▪ Porušenie povinnosti nahlási závažný kybernetický bezpečnostný incident podľa § 24 ods. 1, odoslať neúplné hlásenie podľa § 24 ods. 5 alebo zasielať automatizovaným spôsobom určené systémové informácie podľa § 24a ods. 1, ▪ Porušenie povinnosti riešiť kybernetický bezpečnostný incident na základe rozhodnutia úradu podľa § 27 ods. 3, vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5 alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa § 27 ods. 6, ▪ Porušenie povinnosti predložiť ochranné opatrenie na schválenie alebo vykonať

¹⁹⁷ Celkovým ročným obratom sa na účely ZoKB rozumie súčet všetkých tržieb, výnosov alebo príjmov z predaja tovaru alebo služieb bez nepriamych daní, ku ktorému sa pripočíta poskytnutá finančná pomoc. Obrat vyjadrený v cudzej mene sa prepočíta na eurá, pričom na prepočet cudzej meny na eurá sa použije priemer referenčných výmenných kurzov určených a vyhlásených Európskou centrálnou bankou alebo Národnou bankou Slovenska, ktoré sú platné pre príslušné účtovné obdobie. ZoKB, § 31 ods. 12.

		<p>schválené ochranné opatrenie podľa § 27 ods. 8,</p> <ul style="list-style-type: none"> ▪ Porušenie povinností týkajúcich sa auditu podľa § 29 ods. 1,2 a 5, ▪ Porušenie povinnosti vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29.
Od 300 € do 30 000 €	Poskytovateľovi digitálnej služby	Porušenie povinností podľa § 21 ods. 5 alebo § 23 ods. 2.
Od 300 € až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 €	Poskytovateľovi digitálnej služby	<ul style="list-style-type: none"> ▪ Porušenie oznamovacích povinností podľa § 21 ods. 1, ▪ Porušenie povinností týkajúcich sa bezpečnostných incidentov podľa § 22 ods. 3 a 24 ods. 3, ▪ Porušenie povinností týkajúcich sa procesu hlásenia bezpečnostných incidentov podľa § 25 ods. 1 a ods. 2, ▪ Porušenie povinnosti vykonať reaktívne opatrenie na základe rozhodnutia NBÚ podľa § 27 ods. 5.
Od 300 € do 100 000 €	Komukoľvek	<ul style="list-style-type: none"> ▪ Na výzvu úradu neposkytne informácie podľa § 7 ods. 3, ▪ Neposkytne úradu požadovanú súčinnosť alebo informácie podľa § 10a ods. 1, ▪ Používa konkrétny produkt, službu alebo proces v rozpore s § 27a ods. 5.
Od 300 € do 100 000 €	Výrobcovi alebo poskytovateľovi produktov, služieb alebo procesov	Podľa čl. 53 nariadenia (EÚ) 2019/881 vydá EÚ vyhlásenie o zhode, ktoré je v rozpore s požiadavkami ustanovenými v

		Európskom systéme certifikácie kybernetickej bezpečnosti.
Od 300 € do 100 000 €	Výrobcom alebo poskytovateľovi certifikovaných produktov, služieb alebo procesov alebo výrobcovi alebo poskytovateľovi produktov, služieb a procesov, pre ktoré je vydané EÚ vyhlásenie o zhode,	Nezverejní v elektronickej podobe alebo neaktualizuje doplňujúce informácie o kybernetickej bezpečnosti podľa čl. 55 ods. 1 písm. a) až d) nariadenia (EÚ) 2019/881.
Od 300 € do 100 000 €	Orgánu posudzovania zhody, držiteľovi európskeho certifikátu kybernetickej bezpečnosti alebo vydavateľovi EÚ vyhlásení o zhode	<ul style="list-style-type: none"> ▪ Neposkytne vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti informácie potrebné na plnenie svojich úloh podľa čl. 58 ods. 8 písm. a) nariadenia (EÚ) 2019/881, ▪ Znemožní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti viesť vyšetrovanie v podobe auditu podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.
Od 300 € do 100 000 €	Orgánu posudzovania zhody alebo držiteľovi európskeho certifikátu kybernetickej bezpečnosti,	Neumožní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti prístup do priestorov podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881.

NBÚ je pri ukladaní pokuty povinný prihliadnuť na závažnosť správneho deliktu, najmä na spôsob jeho spáchania, trvanie, následky a na okolnosti, za ktorých bol spáchaný.¹⁹⁸ NBÚ môže uložiť pokutu do dvoch rokov odo dňa zistenia porušenia povinnosti, najneskôr však do štyroch rokov odo dňa, keď k porušeniu povinnosti došlo.¹⁹⁹

3.6.2. Zákon o informačných technológiách vo verejnej správe

ZoITVS upravuje ukládanie sankcií v rámci § 29, kde je riešené ukládania správnych pokút. Správne pokuty môže uložiť orgán vedenia v štyroch kategóriách.

Výška pokuty	Porušenie
Od 500 do 35 000 €	<u>Správcomi za</u> <ul style="list-style-type: none"> ▪ Porušenie základných povinností podľa § 6, ▪ Porušenie povinnosti zabezpečenia plynulej, bezpečnej a spoľahlivej prevádzky IT vo verejnej správe podľa § 12 ods. 1 písm. a), ▪ Porušenie povinnosti nastavenia zmluvných vzťahov s dodávateľmi podľa § 14 ods. 6, ▪ Porušenie povinností pri obstarávaní projektov vo fáze prípravy podľa § 15 ods. 2, ▪ Porušenie povinností týkajúcich sa dojednaní zmluvných podmienok riešenia servisných požiadaviek podľa § 16 ods. 3 písm. e) v spojitosti s § 15 ods. 2 písm. d), ▪ Porušenie povinnosti na úseku bezpečnosti informačných technológií verejnej správy podľa § 19 až 21 alebo § 23.
Od 250 do 35 000 €	<u>Správcomi za:</u> <ul style="list-style-type: none"> ▪ Porušenie vybraných povinností správcov podľa § 12 ods. 1 písm. b), g), h), ▪ Porušenie povinnosti vypracovať koncepciu rozvoja podľa § 13, ▪ Porušenie povinnosti aktualizovať koncepciu rozvoja podľa § 14 ods. 3.

¹⁹⁸ ZoKB, § 31 ods. 10.

¹⁹⁹ ZoKB, § 31 ods. 14.

	<u>Prevádzkovateľovi ITVS za:</u> Porušenie povinnosti týkajúcich sa elektronického odpisu a výstupu z informačného systému verejnej správy.
Od 250 do 25 000 €	<u>Správcovi za</u> <ul style="list-style-type: none"> ▪ Porušenie povinnosti týkajúcich sa sprístupňovania, údajov, dokumentov alebo informácií podľa § 12 ods. 1 písm. e) alebo f), ▪ Porušenie povinnosti dodržiavať štandardy. <u>Orgánu riadenia za</u> <ul style="list-style-type: none"> ▪ Neposkytnutie súčinnosti podľa § 8 ods. 2, ▪ Porušenie povinností týkajúce sa číselníkov podľa § 12 ods. 1 c) a j), ▪ Porušenie povinností týkajúcich sa rozdelenia projektov a ich schválení podľa 15 ods. 4 d) a e), ▪ Porušenie povinností týkajúcich sa predloženia veľkej servisnej požiadavky a jej schváleniu podľa § 16 ods. 3 písm. d).
Od 125 do 500 €	<u>Orgánu riadenia alebo osvedčujúcej osobe:</u> Porušenie inej povinnosti ako uvedených vyššie.

Ukladanie správnych pokút musí orgán vedenia prihliadnuť na „závažnosť, spôsob, trvanie a následky protiprávneho konania, na opakované porušenie povinností alebo na porušenie viacerých povinností. Od uloženia pokuty možno upustiť, ak s prihliadnutím na okolnosti podľa prvej vety postačí na nápravu samotné prejednanie správneho deliktu.“²⁰⁰ Pokutu možno uložiť do troch rokov odo dňa porušenia povinnosti.²⁰¹ ZoITVS neobsahuje ustanovenia previazanosti so Správnym poriadkom pri ukladaní správnych pokút, avšak v zásade tento aspekt nemusí predstavovať problém a predstavuje iba potenciálne zvýšenie právnej istoty pre adresátov právnych noriem.²⁰²

²⁰⁰ ZoITVS, § 29 ods. 2.

²⁰¹ ZoITVS, § 29 ods. 5.

²⁰² Bližšie pozri napr. POTÁŠCH, P. a kol.: *Správny poriadok*. Komentár. 3. vydanie. Praha: C. H. Beck, 2019, § 1.

3.6.3. Identifikované problémy a návrhy riešení

Z vyššie uvedeného porovnania vyplývajú viaceré závery. V prvom rade, samotný typ sankčných oprávnení je inak koncipovaný v ZoKB a ZoITVS. Kým správne pokuty sú súčasťou oboch právnych rámcov, NBÚ ako príslušný orgán v zmysle ZoKB disponuje aj ďalšími oprávneniami ako blokovanie webov alebo oprávnenie zakázať určitý produkt alebo službu. V prípade § 27a (zákazu používať produkt, proces, službu alebo tretiu stranu) je nutné poznamenať, že v zmysle dôvodovej správy ide o *„krajné riešenie v prípadoch, kedy absentujú iné zákonné možnosti zabezpečenia a realizácie kybernetickej bezpečnosti...a ustanovenie je pokračovaním implementácie EÚ Toolbox.“*²⁰³ To, že podobné opatrenie nie je v ZoITVS je síce možné odôvodniť prísnejšími požiadavkami únievého práva alebo usmernení, avšak ak je cieľom zblížovanie právnych rámcov v oblasti kybernetickej bezpečnosti, nemožno niektorým orgánom dané opatrenia dať a niektorým nie. Totožné konštatovanie ale neplatí pre inštitút blokovania, keďže tu by bola právna úprava zjavne duplicitná, nakoľko sa inštitút blokovania neviaže na prevádzkovateľov základných služieb alebo poskytovateľov digitálnych služieb, ale všeobecne na akýkoľvek subjekt.

Zároveň je potrebné poznamenať, že aj výška správnych pokút by mala byť čo najviac zosúladená v daných právnych rámcoch. Prirodzene rozumieme, že množina subjektov podľa ZoITVS a ZoKB nie je kvalitatívne na rovnakej úrovni (napríklad obec a prvok kritickej infraštruktúry), ale základné sadzby podľa týchto zákonov nie sú až tak odlišné. Výnimkou sú pokuty za porušenie povinnosti podľa Aktu o kybernetickej bezpečnosti.

Taktiež je potrebné poznamenať, že lehota na zánik zodpovednosti za správne delikty je odlišná. Pri ZoKB ide o 4 roky, pri ZoITVS sú to len 3 roky. Tieto lehoty by mali byť zosúladené.

²⁰³ ZoKB, Dôvodová správa.

4. KONCEPČNÉ NÁVRHY A ALTERNATÍVY RIEŠENÍ IDENTIFIKOVANÝCH PROBLÉMOV

V predchádzajúcej časti sme identifikovali konkrétne problematické oblasti týkajúce sa regulácie kybernetickej bezpečnosti v Slovenskej republike. Na tieto oblasti sme koncipovali aj návrhy konkrétnych opatrení, ktoré však súviseli vždy s analyzovanou oblasťou. V tejto časti si dovoľíme uviesť niekoľko možností, ktoré sa týkajú koncepcie budúcej regulácie kybernetickej bezpečnosti, ich výhod a nevýhod. Závažným faktorom, ktorý koncepčné riešenia ovplyvňuje je legislatívny vývoj na úrovni EÚ, kde koncom mája došlo k politickej dohode na Smernici NIS 2. Právo EÚ tak naďalej bude zásadne formovať právny rámec kybernetickej bezpečnosti.

Všeobecné alternatívy riešení možno sumarizovať nasledovne:

- 1. Ponechať status quo;**
- 2. Koncipovanie komplexnej právnej úpravy v jednom zákone;**
- 3. Ponechať dva zákony a novelizovať ich s cieľom čo najväčšej previazanosti**

4.1 Ponechať status quo

Prvou možnosťou je ponechať právnu úpravu kybernetickej bezpečnosti v nezmenenom znení a nerobiť žiadne novelizačné kroky. Táto možnosť je podľa nášho názoru najmenej vhodná. V predchádzajúcich častiach analýzy sme poukázali na desiatky nedostatkov právnej úpravy a ich nie vždy vhodnej previazanosti. V súčasnosti daná právna úprava netvorí homogénny celok právnej úpravy kybernetickej bezpečnosti.

Navyše, adresáti povinností v zmysle ZoKB a ZoITVS častokrát nevedia, ktorá právna úprava sa na nich vzťahuje, čo spôsobuje právnu neistotu. Konzervovanie súčasného právneho stavu vzhľadom na vytýkané nedostatky súčasnej právnej úpravy dôrazne neodporúčame.

4.2 Koncipovanie komplexnej právnej úpravy v jednom zákone

Druhou možnosťou, ktorá sa prirodzene núka je koncipovanie právnej úpravy kybernetickej bezpečnosti v jednom zákone, ktorý by bol komplexný a odzrkadľoval potrebu transpozície Smernice NIS a zároveň riadenia informačných technológií verejnej správy z pohľadu politik Slovenskej republiky.

Takýto postup so sebou nesie viaceré riziká, ale aj výhody. Nespornou výhodou by bolo, že adresáti právnych noriem by nemuseli riešiť komplikovanú pôsobnosť dvoch právnych úprav, ako je tomu dnes. Všetky právne informácie by pri takomto riešení našli v jednom zákone a nadväzujúcich podzákonných právnych predpisoch. Ďalšou výhodou je, že ak sme v predchádzajúcich častiach vytýkali niektoré nedostatky v podobe nedostatočných previazaní (napríklad pri sankciách či právomoci dozorných orgánov), tieto by bolo možné jednoducho komplexnou právnou úpravou odstrániť, nakoľko

by legislatívne bolo jednoduchšie nastaviť právomoci dozorných orgánov a nadväzujúcich povinností adresátov právnych noriem v jednotnej podobe.

Nevýhodou komplexnej právnej úpravy je, že sa môže stratiť cieľ jednotlivých právnych úprav, ktorý je pri ZoKB a ZoITVS jemne odlišný. Kým základným cieľom podľa Smernice NIS je prijať „opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci Únie s cieľom zlepšiť fungovanie vnútorného trhu,“ právna úprava informačných technológií vo verejnej správe sa výslovne zameriava iba na správu a riadenie informačných technológií v tomto sektore. Táto „prekážka“ by sa ale mala dať pomerne jednoducho preklenúť hlavne po revízií právnej úpravy v Smernici NIS 2, kde je sektor verejná správa explicitne upravený. Komplexná právna úprava by tak mohla reflektovať aj špecifiká riadenia a vedenia v oblasti IT vo verejnej správe.

Ďalšou nevýhodou je prirodzene dohľad. Kým podľa ZoKB zabezpečuje dohľad príslušný orgán, ktorým je NBÚ, pri ZoITVS je orgánom dohľadu MIRRI. Ak by existovala komplexná právna úprava, pravdepodobne by nastala situácia, aby sa vybral iba jeden primárny orgán dohľadu nad požiadavkami pre kybernetickú bezpečnosť. To nevylučuje, aby MIRRI ostali niektoré kompetencie pri vedení a riadení IT vo verejnej správe, tie by však mali byť precízne vymedzené, aby nedochádzalo ku kompetenčným konfliktom.

4.3 Ponechať dva zákony a novelizovať ich s cieľom čo najväčšej previazanosti

Z krátkodobého hľadiska je výhodnou možnosťou ponechať dve právne úpravy a odstrániť v nich nezrovnalosti, na ktoré sme poukázali najmä v tretej časti predkladanej analýzy. Rozumieme, že z hľadiska adresátov právnych noriem nepôjde o preferovanú možnosť. Berieme však do úvahy prípadne dlhé negociácie medzi gestormi ZoKB a ZoITVS pri potenciálnej tvorbe jedného zákona, ktorý by reguloval oblasť kybernetickej bezpečnosti. Zároveň, by na takýto krok musela byť politická vôľa. Z tohto pohľadu sa javí ako najschodnejšie riešenie novelizovať ZoKB a ZoITVS takým spôsobom, aby boli čo najviac previazané a nespôsobovali by interpretačné problémy. Skutočne by sa tak vytvoril komplexný právny rámec regulácie kybernetickej bezpečnosti v Slovenskej republike.

Za nevyhnutné minimum považujeme odstránenie nasledujúcich nedostatkov, pričom ich odôvodnenie je možné nájsť v tretej kapitole:

- Vyriešiť komplikovanú pôsobnosť týkajúcu sa subjektov podľa ZoKB a ZoITVS,
- Zjednotiť výklad základných pojmov v oblasti kybernetickej bezpečnosti,
- Zjednotiť nahlásovanie bezpečnostných incidentov,
- Zjednotiť bezpečnostné opatrenia,
- Odstrániť problémy súvisiace so zlou transpozíciou Smernice NIS,
- Čo najviac priblížiť oprávnenia dozorných a príslušných orgánov podľa ZoKB a ZoITVS,

- Konceptne uchopiť transpozíciu Smernice NIS 2 po prijatí finálneho textu.

Odstránenie vyššie uvedených nedostatkov je iba malým krokom v oblasti regulácie. Máme za to, že ak z krátkodobého alebo strednodobého hľadiska budú v Slovenskej republike platiť dva zákony, je potrebné urobiť aj nepriame opatrenia, ktoré budú opakovane zvyrazňovať a vysvetľovať právny rámec. Víťame ambiciózne ciele Slovenskej republiky v rámci Plánu obnovy a odolnosti, ktorý strategicky podporuje zvýšenie vzdelávania v oblasti kybernetickej bezpečnosti na všetkých stupňoch, zriaďovanie kompetenčných centier či investície do infraštruktúry. Práve toto sú opatrenia, ktoré približujú oblasť kybernetickej bezpečnosti adresátom právnych noriem a laickej verejnosti a zároveň upriamujú pozornosť na reguláciu.

PRÍLOHA
ZOZNAM NÁVRHOV A OPATRENÍ

#	Monitoring právnych predpisov
1.	Monitorovať legislatívne procesy týkajúce sa nových strategických dokumentov a regulácie digitálneho trhu EÚ z dôvodu identifikovania potenciálnych konfliktných oblastí v legislatíve.
2.	Monitorovať proces prijatia Európskeho vyhlásenia o digitálnych právach a zásadách v digitálnom desaťročí s ohľadom na záväzky v oblasti kybernetickej bezpečnosti.
3.	Pri komunikovaní usmernení a odporúčaní pre bezpečnostné opatrenia v zmysle ZoKB alebo ZoITVS je potrebné upriamiť pozornosť aj na otázky článku 32 GDPR. Považujeme to za nevyhnutné, aby adresáti usmernení alebo odporúčaní mali komplexný obraz o regulácii bezpečnosti.
4.	<p>Nahlasovanie bezpečnostných incidentov a ich modalít je predmetom právnej úpravy viacerých aktov. Menovať môžeme GDPR, zákon o elektronických komunikáciách, ZoKB, ZoITVS, zákon o platbách či nariadenie eIDAS. Je preto viac ako pravdepodobné, že jedna entita bude musieť nahlasovať bezpečnostné incidenty podľa rôznych právnych predpisov.</p> <p>Z pohľadu MIRRI je preto dôležité čo najviac vplývať na úpravu legislatívy tak, aby nahlasovanie bezpečnostných incidentov podľa rôznych právnych predpisov bolo uchopené koncepcne a pokiaľ možné aj jednotne. Minimom by malo byť vzdelávanie a konkrétne odporúčania s metodikami pre nahlasovanie bezpečnostných incidentov pre adresátov noriem v pôsobnosti MIRRI.</p>
5.	Rola DPO je významne previazaná s úlohami manažéra kybernetickej bezpečnosti. Z tohto dôvodu považujeme za nevyhnuté aby MIRRI v rámci vzdelávania v oblasti kybernetickej bezpečnosti zahrnula aj oblasť ochrany osobných údajov. Uvedené je potrebné integrovať aj v rámci metodických usmernení pre orgány verejnej moci z hľadiska bezpečnosti.
6.	Monitorovať proces prijatia aktu o umelej inteligencii a vyhodnocovať vplyv nariadenia na využívanie systémov AI v kritickej infraštruktúre a digitálnej infraštruktúre.
7.	Monitorovať prijímanie štandardov v zmysle Aktu o kybernetickej bezpečnosti pre systémy AI.
8.	Monitorovať prijímanie štandardov v zmysle AIA za predpokladu, že bude platiť prezumpcia správnosti s požiadavkami v legislatíve.
9.	Monitorovať prijímanie DSA a požiadaviek na digitálne služby z hľadiska kybernetickej bezpečnosti. Ak bude zriadený koordinátor digitálnych služieb podľa DSA, MIRRI môže novému subjektu poskytovať cenné know-how a odporúčania pri kontrole požiadaviek na kybernetickú bezpečnosť subjektov v pôsobnosti DSA.
10.	Monitorovať prijímanie revízie Nariadenia eIDAS z hľadiska kybernetickej bezpečnosti.
11.	Monitorovať transpozíciu prijatého Návrhu smernice NIS 2, a to najmä s ohľadom na správnu interpretáciu pojmu subjekt verejnej správy v rámci nového sektora Verejná správa.

12.	Monitorovať transpozíciu prijatého Návrhu smernice NIS 2 a to najmä s ohľadom na bezpečnostné opatrenia, ktoré budú musieť plniť subjekty verejnej správy v rámci nového sektora Verejná správa.
13.	Monitorovať transpozíciu prijatého Návrhu smernice o odolnosti kritických subjektov, a to najmä s ohľadom na správnu interpretáciu pojmu subjekt verejnej správy v rámci nového sektora Verejná správa, ako aj určovania prahových hodnôt v odvetví, resp. pododvetví, kde bude MIRRI príslušným orgánom.
14.	Monitorovať transpozíciu prijatého Návrhu smernice o odolnosti kritických subjektov, a to najmä s ohľadom na určenie parametrov pre určenie závažnosti narušenia prevádzky kritického subjektu.
15.	Iniciovať vyradenie správcov, ktorí sú zaradení v registri PZS v sektore verejná správa a podsektore informačné systémy verejnej správy, pri ktorých sa neskúmali dopadové kritériá.
16.	Aktualizovať zoznam orgánov riadenia uvedená v ustanovení § 3 ods. 4 vyhlášky č. 179/2020 Z. z.
17.	Identifikovať základné služby pre sektor verejná správa a podsektor informačné systémy verejnej správy. Táto úloha dokonca priamo vyplýva z ustanovenia § 9 ods. 1 písm. f) ZoKB, v zmysle ktorého MIRRI v rozsahu svojej pôsobnosti pre sektor verejná správa a podsektor informačné systémy verejnej správy, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá NBÚ na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb.

#	Zákon o kybernetickej bezpečnosti
1.	Koncepčne uchopiť úlohy a právomoci NBÚ pri revízii právneho rámca kybernetickej bezpečnosti.
2.	Koncepčne uchopiť výkon vyšetrovania auditovania pri revízii právneho rámca kybernetickej bezpečnosti.
3.	Koncepčne uchopiť blokovanie webových stránok a pri legislatívnom procese vyzývať na rešpektovanie judikatúry Európskeho súdu pre ľudské práva a Súdneho dvora Európskej únie.
4.	Zabezpečiť pri revízii právneho rámca kybernetickej bezpečnosti precíznejšiu transpozíciu úloh jednotiek CSIRT v oblasti štandardizácie a spolupráce so súkromným sektorom.

#	Zákon o informačných technológiách vo verejnej správe
1.	Definovať pojem bezpečnosť informačných technológií verejnej správy definovať v ZoITVS, resp. odkázať na pojem kybernetická bezpečnosť v zmysle ZoKB.
2.	Zjednotiť terminológiu a doplniť chýbajúce obsahové prvky niektorých dokumentov ako napr. bezpečnostná stratégia kybernetickej bezpečnosti.
3.	Zadefinovať pojem kybernetický bezpečnostný incident pre účely nahlasovania takýchto incidentov správcami, ktorí sú len v jednom právnom postavení.
4.	Stanoviť lehotu na nahlasovanie kybernetických bezpečnostných incidentov, ktoré nie sú závažné na bezodkladne.
5.	Rozšíriť povinnosť nahlasovať kybernetické bezpečnostné incidenty aj na orgány riadenia podľa § 5 ods. 2 písm. c) – h) ZoITVS.
6.	Zabezpečiť pri revízii právneho rámca kvalitnejšiu reflexiu úloh a právomoci orgánu vedenia a upraviť špecifický postup pri výkone kontroly.
7.	V prípade potreby analyzovať potrebu zavedenia auditovania ex offio zo strany orgánu vedenia a prispôbiť týmto záverom právnu úpravu v ZoITVS.