SBA

SLOVAK | BUSINESS | AGENCY

REGULÁCIA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI V EÚ A SR

BRATISLAVA 2025

Vydavateľ: Slovak Business Agency

Obsah

Obsah 3
Zoznam použitých skratiek 5
Manažérske zhrnutie 6
1 Regulačné prostredie na úrovni EÚ 8
1.1 Význam malých a stredných podnikov v hospodárstve SR 10
1.2 História celoeurópskej legislatívy v oblasti kybernetickej bezpečnosti 12
1.3 Smernica Európskeho parlamentu a rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2) 14
1.3.1 Rozsah pôsobnosti 14
1.3.2 Výnimky z rozsahu pôsobnosti 17
1.3.3 Dôležité, kľúčové a iné subjekty 17
1.3.4 Kybernetické hrozby 19
1.3.5 Kybernetická bezpečnosť 20
1.3.6 Dodávateľské reťazce, poskytovatelia dôveryhodných, interpersonálnych, komunikačných služieb a služieb registrácie domén 23
1.3.7 Manažment kybernetických rizík na úrovni podnikateľských subjektov 25
1.3.8 Priebeh a oznamovanie incidentov 26
1.3.9 Dohľad nad subjektami a princípy teritoriality 28
1.3.10 Sankcie 30
1.3.11 Špecifické výzvy pre malé a stredné podniky v kontexte smernice NIS2 31
1.4 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR) 33
1.4.1 Záznamy o spracovateľských činnostiach 34
1.4.2 Porušenia ochrany osobných údajov 35
1.4.3 Posúdenie vplyvu na ochranu údajov 36
1.4.4 Zodpovedná osoba (DPO) 37
1.4.5 Kódexy správania a certifikácia 37
1.4.6 Prenositeľnosť údajov 38
1.4.7 Dozorné orgány a sankcie 39
1.5 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (CSA) 41
1.5.1 Agentúra ENISA 41
1.5.2 Certifikácia kybernetickej bezpečnosti 41
1.6 Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 o jednotnom trhu s digitálnymi službami (DSA) 44
1.6.1 Povinnosti poskytovateľov sprostredkovateľských služieb 44
1.6.2 Dohľad a sankcie 47
1.7 Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA) 48
1.7.1 Riadenie rizík 48
1.7.2 Incidenty súvisiace s IKT 49
1.7.3 Testovanie digitálnej prevádzkovej odolnosti 50
1.7.4 Riadenie externého rizika IKT 51
1.7.5 Dohľad a sankcie 51
1.8 Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (CRA) 52
1.8.1 Povinnosti výrobcov, dovozcov a distribútorov 52
1.8.2 Správa softvérov s otvoreným zdrojovým kódom 53
1.8.3 Označenie o zhode a technická dokumentácia 54
1.8.4 Sankcie 55
2 Regulačné prostredie na úrovni SR 56
2.1 Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti 56
2.1.1 Dohliadajúci orgán 56
2.1.2 Rozsah pôsobnosti 57
2.1.3 Povinnosti poskytovateľov základnej služby 58
2.1.4 Dohľad a sankcie 60
2.2 Národná stratégia kybernetickej bezpečnosti na roky 2021-2025 62
2.3 Najdôležitejšie zmeny pre MSP od 1.1.2025 63

3 Príklady implementácie opatrení v praxi 65
3.1 Pozitívne príklady z iných členských štátov EÚ 65
3.2 Najväčšie výzvy a chyby pri implementácii 68
4 Kvalitatívny prieskum 71
4.1 Formalizácia prístupu ku kybernetickej bezpečnosti 72
4.2 Proces riešenia incidentov 73
4.3 Ochrana dát 74
4.4 Najväčšie vnímané hrozby 75
4.5 Skúsenosti s narušením bezpečnosti 75
4.6 Vnímanie roly štátu 76
4.7 Prekážky a možné príležitosti 77
Záver 78
Zoznam použitej literatúry 80

Zoznam použitých skratiek

AI	Umelá inteligencia
CE	Európska zhoda (označenie)
CRA	Nariadenie 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (Akt o kybernetickej odolnosti)
CSIRT	Jednotka pre riešenie kybernetických bezpečnostných incidentov
DORA	Nariadenie 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora **(**Akt o digitálnej prevádzkovej odolnosti)
DNS	Systém názvov domén
DPO	Zodpovedná osoba
DSA	Nariadenie 2022/2065 o jednotnom trhu s digitálnymi službami (Akt o digitálnych službách)
GDPR	Nariadenie 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
HDP	Hrubý domáci produkt
ENISA	Agentúra Európskej únie pre kybernetickú bezpečnosť
EU-CyCLONe	Európska sieť styčných organizácií pre riešenie kybernetických kríz
EÚ	Európska únia
IKT	Informačno-komunikačné technológie
MSP	Malé a stredné podniky
NBÚ	Národný bezpečnostný úrad
NBS	Národná banka Slovenska
NIS2	Smernica 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii
OKÚ	Osobitné kategórie údajov
SR	Slovenská republika
TLD	Doména najvyššej úrovne
WHOIS	Databáza registračných údajov názvov domén

Manažérske zhrnutie

Smernica NIS2, transponovaná do novelizovaného slovenského zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej ako zákon č. 69/2018 Z. z.) sa vzťahuje na tie MSP, ktorých služby sú považované za základné (kritické) pre hospodárstvo krajiny alebo EÚ. Zákon č. 69/2018 Z. z. pokrýva množstvo sektorov naprieč celým hospodárstvom. Vzhľadom k tomu, že väčšina domácich podnikateľských subjektov (až 98,8 %) pochádza z prostredia MSP, je možné s určitosťou tvrdiť, že mnohé z nich, nech už pôsobia v akomkoľvek sektore, budú spadať do pôsobnosti tohto zákona a musia tak dodržiavať zákonom dané bezpečnostné opatrenia.

Poskytovatelia špecifických služieb (online sprostredkovanie, IKT, finančné služby, produkty s digitálnymi prvkami, databázy) sa musia okrem zákona č. 69/2018 Z. z. riadiť aj špeciálnymi odvetvovými aktami, ktoré upresňujú ich povinnosti vo vzťahu k zabezpečeniu kybernetickej bezpečnosti. Akty CRA, CSA, DSA, DORA alebo nariadenie GDPR sú pre takýchto poskytovateľov zároveň primárnym zdrojom povinností a zákon ich len dopĺňa.

Manažment je povinný zabezpečiť dodržiavanie požiadaviek zákona (alebo odvetvových aktov) a môže niesť právnu zodpovednosť za nedodržanie opatrení. Za neplnenie povinností vyplývajúcich zo zákona (alebo odvetvových aktov) hrozia podnikom vysoké pokuty a v krajnom prípade aj pozastavenie poskytovania služieb.

Podniky sú povinné riadiť riziká prostredníctvom zavedenia opatrení na minimalizáciu kybernetických hrozieb, ako sú napr. bezpečnostné politiky, zálohovanie dát, šifrovanie, kontrola prístupu, alebo reakčné plány na incidenty. Zákon vyžaduje, aby podniky dôkladne kontrolovali dodávateľov a spolupracujúce subjekty, tak aby obmedzili možnosť kybernetického útoku cez dodávateľský reťazec. Podniky sú podľa zákona povinné nahlásiť významné bezpečnostné incidenty do 24 hodín, s následnou aktualizáciou do 72 hodín a záverečnou správou do mesiaca.

Slovenský dohliadajúci orgán, ktorým je NBÚ, vytvoril pre dotknuté podniky pomoc so sebaidentifikáciou, registráciou, informovaním a pre nahlasovanie incidentov a hrozieb online webové rozhrania (resp. štandardizované tlačivá).

Podľa nariadenia GDPR sú všetky podniky povinné zabezpečiť ochranu osobných údajov svojich zákazníkov, zamestnancov aj obchodných partnerov. Ak MSP spracúvajú citlivé údaje alebo pravidelne spracúvajú osobné údaje, musia si viesť evidenciu svojich spracovateľských činností.

Certifikáty kybernetickej bezpečnosti nie sú podľa odvetvového aktu CSA pre MSP podnikajúce v oblastiach digitálnych produktov a služieb povinné. Ich vlastníctvo ale môže MSP poskytovať na trhu konkurenčnú výhodu. MSP môžu využiť finančne prístupnejšiu formu modulárnych certifikácií (základný certifikát + nadstavby podľa potreby/možností).

MSP, ktoré vyvíjajú, predávajú alebo distribuujú digitálne produkty musia podľa aktu CRA zabezpečiť ich odolnosť voči kybernetickým hrozbám, a to najmenej po dobu 5 rokov. Vysokorizikové produkty naviac podliehajú povinnej certifikácií.

Podľa odvetvového aktu DSA musia MSP prevádzkujúce online trhoviská overovať totožnosť predajcov. Odvetvový akt DSA zavádza pre všetky podniky prísnejšie pravidlá zverejňovania online reklamy.

MSP, ktoré pôsobia vo finančných službách alebo spolupracujú s finančnými inštitúciami musia podľa odvetvového aktu DORA zabezpečiť odolnosť svojich produktov, služieb a systémov voči kybernetickým útokom alebo výpadkom systému. Môžu sa na ne tiež vzťahovať

požiadavky na vykonávane bezpečnostných testovaní, auditov kybernetickej bezpečnosti alebo hodnotenia odolnosti.

Všetky právne normy umožňujú malým podnikom úľavy z niektorých povinností, napr. podávanie menej detailných reportov alebo uplatňovanie zjednodušených postupov. Zároveň je na základe riadených diskusií s predstaviteľmi MSP možné zhodnotiť ich pripravenosť čeliť kybernetickým hrozbám za nedostatočnú, a to najmä z dôvodu nedostatku zdrojov, ktoré do tejto oblasti smerujú. Kybernetické hrozby na druhej strane vnímajú ako reálne a v niektorých prípadoch sa stretli s útokom zameraným na ich podnik. Každopádne čím abstraktnejšia je pre MSP hrozba (pretože podnik nemá vlastnú negatívnu skúsenosť a nevenuje pozornosť, resp. k nemu neprichádza dostatok informácií o hrozbách), tým menší dôraz kladie na oblasť ochrany.

Kľúčovým nástrojom štátu pre docielenie väčšej miery odolnosti a súladu s reguláciou je komunikácia, vo všetkých vhodných formách. Podnikom samozrejme dokáže pomôcť ďalšími praktickými pomôckami (rozhrania pre reportovanie incidentov, identifikáciu subjektov a pod.), zrozumiteľné a včasné informácie sú ale základom úspešnej implementácie.

1 Regulačné prostredie na úrovni EÚ

S kumulatívnym HDP všetkých členských krajín na úrovni 17 biliónov EUR patrí Európska únia medzi najväčšie hospodárstva sveta. Ako jeden z najbohatších ekonomických celkov sa stáva v globálnej interakcii prirodzeným partnerom pre výmenu tovarov, služieb, ako aj informácií a know-how. Bohatnúca európska spoločnosť sa mení aj socio-demograficky, čo so sebou prináša zmeny spoločenských modelov, premietajúcich sa následne do politiky jednotlivých štátov, ale aj EÚ ako celku.

Globálne obchodovanie a politika so sebou však prirodzene prinášajú aj výzvy, často siahajúce až za hranice férovej hospodárskej a politickej súťaže.

Na úrovni obchodovania a finančných tokov sú to najčastejšie nelegálne aktivity štátnych aj neštátnych subjektov z krajín mimo EÚ, vedúce k získaniu know-how, databáz, komunikácie alebo priameho prístupu k finančným tokom európskych spoločností. Mimoeurópskych ekonomických aktérov často zaujíma aj koncový európsky zákazník a jeho socio-demografický profil a nákupné správanie, s cieľom získať na vnútornom trhu EÚ konkurenčnú výhodu. Samostatnou kapitolou je celé spektrum kriminálnych aktivít vedúcich od získania prístupu k finančným zdrojom obete, cez krádeže identity osôb, až po činnosť narúšajúcu súkromie a osobnú integritu človeka.

Rapídne narastajúcim problémom, predovšetkým v poslednom desaťročí, je činnosť štátnych aktérov (alebo ich proxy-subjektov spomedzi iných štátnych aj neštátnych hráčov). Krajiny neschopné uspieť v štandardnej hospodárskej súťaži s EÚ alebo naopak krajiny, ktoré sa profilujú ako globálny vyzývateľ EÚ na poli ekonomiky, politicko-spoločenského zriadenia a hodnôt sa už neuchyľujú len k vyššie uvedenému získavaniu citlivých informácií, ale čoraz častejšie aj k priamemu narúšaniu energetických, finančných, informačných a dopravných tokov, ako aj základných služieb pre obyvateľov EÚ. Realizáciou podobných opatrení tzv. hybridnej vojny je tak narúšaná nielen dôvera občanov v štát a Európsku úniu, ale postupne tak dochádza hlavne k rozpadu súdržnosti a hodnôt spoločnosti. V globálnej politickej a ekonomickej súťaži dochádza k oslabovaniu EÚ (a jednotlivých členských štátov) na úkor jej vyzývateľov, väčšinou spomedzi krajín s nedemokratickým politicko-spoločenským zriadením.

Tieto hrozby sú o to naliehavejšie, čím viac sa ekonomický život, riadiace systémy, ale aj zdieľanie citlivých osobných údajov prenáša do virtuálneho prostredia. Po narastajúcom množstve bezpečnostných incidentov, ktorých cieľom sa stávajú spoločnosti a jednotlivci s domicilom v EÚ, ale predovšetkým vzhľadom k narastajúcemu počtu incidentov súvisiacich s kritickou infraštruktúrou, pristúpila Európska komisia k vypracovaniu viacerých právnych aktov reflektujúcich oblasť regulácie kybernetickej bezpečnosti. Svojím obsahom adresujú:

- **Zvyšujúcu sa závislosť od digitálnych technológií** - v dnešnom svete sú digitálne technológie neoddeliteľnou súčasťou nášho života. Od bankovníctva a zdravotníctva až po dopravu a energetiku – všetko je stále viac prepojené a závislé na digitálnych systémoch. Táto závislosť však so sebou prináša aj zvýšené riziko kybernetických útokov.
- **Globálny charakter kybernetických hrozieb** - kybernetické hrozby môžu pochádzať odkiaľkoľvek na svete a môžu mať vplyv na celé odvetvia či dokonca na celú spoločnosť. Z tohto dôvodu je potrebná koordinovaná reakcia na európskej úrovni.
- **Ochranu občanov a spoločností so sídlom v EU** - kybernetické útoky majú vážne dôsledky pre jednotlivcov, podniky a štáty. Môžu viesť k finančným stratám, strate dát, narušeniu prevádzky a poškodzovať goodwill. Regulácia má za cieľ chrániť občanov a podniky pred týmito hrozbami.
- **Budovanie a zvyšovanie dôvery v digitálny trh** - jasné a jednotné pravidlá v oblasti kybernetickej bezpečnosti zvyšujú dôveru v digitálny trh. Podniky môžu ľahšie identifikovať a

zmierňovať riziká spojené s kybernetickými hrozbami, čo vedie k zvýšeniu ich konkurencieschopnosti.

- **Ochranu kritickej infraštruktúry** - kybernetické útoky na kritickú infraštruktúru, ako sú energetické siete, zdravotnícke zariadenia alebo dopravné systémy, môžu mať vážne dôsledky pre spoločnosť. Regulácia zabezpečuje, aby bola kritická infraštruktúra dostatočne chránená.

Hlavnými cieľmi regulácie kybernetickej bezpečnosti v Európskej únií sú:

- **Harmonizácia právnych predpisov** - cieľom je vytvoriť jednotný právny rámec pre kybernetickú bezpečnosť v celej EÚ, čo zjednoduší podnikanie a zvýši právnu istotu.
- **Zvýšenie odolnosti** - regulácia má za cieľ zvýšiť odolnosť európskych systémov voči kybernetickým útokom.
- **Podpora spolupráce** - očakáva sa vytvorenie kooperačných programov medzi členskými štátmi, súkromným sektorom a akademickou obcou v oblasti kybernetickej bezpečnosti.
- **Zvýšenie povedomia** - regulácia prispieva k zvýšeniu povedomia o kybernetických hrozbách a dôležitosti ochrany osobných údajov.

1.1 Význam malých a stredných podnikov v hospodárstve SR

Malé a stredné podniky (ďalej MSP) sú podnikateľské subjekty, ktoré Európska komisia rozdeľuje a definuje na základe kritérií počtu zamestnancov, obratu alebo bilančnej sumy. Mikropodniky sú podľa tejto definície tie, ktoré majú menej ako 10 zamestnancov a ročný obrat alebo bilančnú sumu do 2.000.000,- EUR.

Malé podniky zamestnávajú do 50 pracovníkov a majú ročný obrat alebo bilančnú sumu do 10.000.000,- EUR. Stredné podniky majú menej ako 250 zamestnancov a ročný obrat do 50.000.000,- EUR alebo bilančnú sumu do 43.000.000,- EUR.

MSP zohrávajú v hospodárstve SR významnú úlohu. Podľa zatiaľ poslednej správy SBA o malom a strednom podnikaní na Slovensku[1] za rok 2023, tento typ podnikateľských subjektov zastupuje 98,8 % spomedzi všetkých v tuzemsku registrovaných firiem.

Celkovo bolo v roku 2003 v SR registrovaných 666.928 MSP, z toho malých podnikov bolo 13.674 (asi 2,0 % všetkých podnikateľských subjektov v SR) a stredných podnikov 2.731 (asi 0,4 % všetkých podnikateľských subjektov v SR). Výrazne dominujú mikropodniky, ktorých bolo 650.533 (asi 97,4 % všetkých podnikateľských subjektov v SR).

Z hľadiska právnej formy MSP tvoria 60,5 % fyzické osoby – podnikatelia a 39,5 % právnické osoby. Výrazná väčšina MSP – až 88,8 % - je v domácom súkromnom vlastníctve, 9,8 % MSP má zahraničných súkromných vlastníkov a len 1,0 % má medzinárodnú vlastnícku štruktúru. Iný typ vlastníctva (napr. družstevné, štátne) má zostávajúcich 0,4 % MSP.

Štruktúra odvetví, ktorým sa MSP venujú, pokrýva väčšinu činností v slovenskom hospodárstve. Najčastejším odvetvím podnikania MSP sú obchodné služby (27 %), ktoré sú zároveň doménou stredných podnikov. Stavebníctvo (19,5 %) je najčastejším druhom podnikania medzi mikropodnikmi. Nasledujú obchod (15,2 %) a priemysel (13,4 %), v ktorom sú najčastejšie zastúpené stredné podniky. Podiely ostatných odvetví na podnikaní MSP sú už nižšie ako 10 % - doprava, informačné a komunikačné činnosti (9,2 %), ostatné služby (8,1 %), pôdohospodárstvo (3,7 %) a ubytovanie a stravovanie (3,1 %).

Medzi MSP, angažujúcimi sa v odvetviach s vysokou technologickou úrovňou nájdeme najčastejšej podnikateľské subjekty z odvetvia high-tech služieb (počítačové programovanie, poradenstvo a súvisiace služby).

Najviac MSP má sídlo v Bratislavskom kraji – až 23,2 % subjektov. Naopak, najmenšie zastúpenie vykazujú Trenčiansky a Banskobystrický kraj, kde je spomedzi všetkých slovenských MSP usadených len 9,1 % subjektov.

MSP v roku 2023 zamestnávali 1.419.500 osôb, čo je podiel 59,2 % na celkovej zamestnanosti v hospodárstve SR.

Najvyšší podiel tržieb pripadá na MSP v odvetví služieb – až 74,2 % z celkových tržieb sektoru za rok 2023. Vysoký podiel majú MSP aj na stavebnej produkcií (t. j. hodnote vykonaných stavebných prác), a to konkrétne 86,3 %.

Exportné aktivity za rok 2023 sa na celkovom vývoze podieľali 28,4 % (v úhrnnej sume 23.590.000.000,- EUR**),** z toho mikropodniky 7,4 %, malé podniky 7,0 % a stredné podniky 14,1 %. Výrazná väčšina vývozu MSP smerovala do krajín EÚ (86,8 %), pričom dominantnými exportovanými komoditami boli stroje, prístroje a elektronické zariadenia.

[1] Detailné informácie je možné nájsť v správe Malé a stredné podnikanie v číslach v roku 2023 https://monitoringmsp.sk/wp-content/uploads/2024/05/MSP_v_cislach_2023.pdf

Podiel MSP na celkovom dovoze v roku 2023 bol 37,3 % (v úhrnnej sume 35.314.900.000,- EUR). Až 75,8 % komodít dovezených MSP na Slovensko pochádzalo z EÚ.

Z hľadiska využívania IKT, čo má priamy súvis práve s kybernetickou bezpečnosťou, mali v roku 2023 slovenské MSP tieto kľúčové parametre:

- prístup na internet mali zamestnanci v 92,7 % malých podnikov a 93,0 % stredných podnikov,
- webové sídlo (stránku) malo 74,3 % malých podnikov a 83,1 % stredných podnikov,
- na online objednávanie a rezervovanie využívalo svoje webové sídlo 32,8 % malých podnikov a 27,6 % stredných podnikov,
- na prezentáciu tovarov a služieb využívalo svoje webové sídlo 90 % MSP,
- na predaj využívalo svoje webové sídlo 16,8 % malých podnikov a 21,2 % stredných podnikov,
- sociálne média využívalo pri podnikaní 46,1 % malých podnikov a 54,2 % stredných podnikov,
- služby cloud-computingu využívalo pri podnikaní 32,4 % malých podnikov a 49,9 % stredných podnikov. V tomto ukazovateli išlo najčastejšie o aplikácie elektronickej pošty (90,8 % MSP). bezpečnostné softvérové aplikácie (75,7 % MSP) a kancelárske aplikácie (70 % MSP).

Z uvedeného prehľadu je zrejmé, že MSP zasahujú prakticky do každého odvetvia hospodárstva. Je preto dôležité uvedomiť si, že na nezanedbateľnú časť malých a stredných podnikov sa vzťahuje aj legislatíva regulujúca oblasti kybernetickej bezpečnosti a súvisiacich problematík.

1.2 História celoeurópskej legislatívy v oblasti kybernetickej bezpečnosti

Prvým právnym aktom Európskeho parlamentu v oblasti kybernetickej bezpečnosti bola smernica 2002/58/ES o spracovávaní osobných údajov a ochrane súkromia v sektore elektronických komunikácií, vydaná v roku 2002. Táto smernica stanovila pravidlá pre spracovanie osobných údajov v elektronickom styku a uložila členským štátom povinnosť zaviesť vnútroštátne právne predpisy na jej vykonanie.

V roku 2013 Európska komisia vydala nariadenie 526/2013 o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií, ktoré stanovilo rámec pre spoluprácu medzi členskými štátmi v oblasti kybernetickej bezpečnosti. Nariadenie tiež zriadilo Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA), ktorá má za úlohu pomáhať členským štátom pri riešení problémov v tejto oblasti.

V roku 2016 Európska únia prijala smernicu 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (NIS), ktorá uložila členským štátom povinnosť zaviesť vnútroštátne stratégie kybernetickej bezpečnosti a zriadiť národné orgány pre kybernetickú bezpečnosť. Smernica NIS tiež uložila prevádzkovateľom dôležitých služieb, ako sú napríklad energetika, doprava a financie, povinnosť prijať bezpečnostné opatrenia na ochranu svojich sietí a informačných systémov.

V rovnakom roku bolo tiež prijaté nariadenie č. 2016/279 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov . Nariadenie sa vzťahuje aj na kybernetickú bezpečnosť, pretože ukladá prevádzkovateľom povinnosť prijať bezpečnostné opatrenia na ochranu osobných údajov pred neoprávneným prístupom alebo zneužitím.

V roku 2019 bolo prijaté nariadenie č. 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (neformálne známe ako „Akt o kybernetickej bezpečnosti“). Ide o komplexný právny rámec, ktorý sa snaží posilniť kybernetickú bezpečnosť v EÚ prostredníctvom širších právomocí pre agentúru ENISA, zavedenia certifikačných systémov, podpory spolupráce a výmeny informácií, budovania kapacít a zlepšenia reakcie na incidenty.

V roku 2020 Európska komisia predstavila novú stratégiu kybernetickej bezpečnosti EÚ, ktorá stanovila ciele a opatrenia pre posilnenie kybernetickej bezpečnosti v Európskej únii. Stratégia sa zamerala na tri hlavné oblasti:

- zvýšenie odolnosti európskej spoločnosti a ekonomiky voči kybernetickým útokom,
- posilnenie spolupráce medzi členskými štátmi a inštitúciami EÚ v oblasti kybernetickej bezpečnosti,
- podpora rozvoja európskeho priemyslu kybernetickej bezpečnosti.

V roku 2022 bolo prijaté rozsiahle nariadenie 2022/2065 o jednotnom trhu s digitálnymi službami (neformálne označované ako „Akt o digitálnych službách“ (DSA)). Zameriava sa na reguláciu online platforiem a sprostredkovateľských služieb v digitálnom priestore. Jeho cieľom je vytvoriť bezpečnejšie a spravodlivejšie online prostredie pre používateľov a podniky.

V rovnakom roku (2022) bolo prijaté aj nariadenie 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (neformálne známe ako „Akt o digitálnej prevádzkovej odolnosti“ (DORA). Jeho cieľom je zabezpečiť, aby finančné inštitúcie a kritickí poskytovatelia info-komunikačných služieb boli schopní odolať, reagovať a zotaviť sa z narušení prevádzkovaných systémov.

Tretím dokumentom prijatým v roku 2022 bola aktualizácia smernice NIS z roku 2016. Nová smernica 2022/2555. Smernica NIS2 v porovnaní s jej predchádzajúcou verziou rozširuje

škálu subjektov, na ktoré sa vzťahuje, zavádza prísnejšie požiadavky na riadenie rizík a oznamovanie incidentov a výraznejšie posilňuje spoluprácu medzi členskými štátmi EÚ v oblasti kybernetickej bezpečnosti.

Zatiaľ posledným prijatým dokumentom z tejto oblasti je nariadenie 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (známe ako „Akt o kybernetickej odolnosti“ – CRA). Nariadenie sa zameriava na zvýšenie kybernetickej bezpečnosti produktov s digitálnymi prvkami, čiže hardvéru a softvéru, ktoré sú pripojené k internetu.

V najbližších rokoch sú pripravované aj ďalšie **nariadenia**, ktoré sa viac či menej dotýkajú kybernetickej bezpečnosti. Menovať je možné napríklad **„Akt o umelej inteligencií“ (AI Act)**, ktorý bude obsahovať aj dôležité ustanovenia týkajúce sa kybernetickej bezpečnosti systémov umelej inteligencie. Ďalším pripravovaným dokumentom je aj **Európsky rámec pre digitálnu identitu**, ktorého cieľom je vytvoriť bezpečný a interoperabilný systém digitálnej identity pre občanov a podniky v EÚ, tak aby mohli bezpečne a jednoducho preukazovať svoju totožnosť online a pristupovať k digitálnym službám. Do tretice sa očakáva zmena **nariadenia o agentúra ENISA**, tak aby mohla efektívnejšie plniť svoje úlohy v oblasti kybernetickej bezpečnosti.

Okrem týchto nariadení EÚ pripravuje aj rôzne stratégie a iniciatívy, ktoré majú za cieľ v rôznych oblastiach posilniť kybernetickú bezpečnosť. Patria medzi ne napríklad:

- Aktualizovaná **Stratégia kybernetickej bezpečnosti EÚ** - nová stratégia stanoví dlhodobé ciele a priority EÚ v oblasti kybernetickej bezpečnosti.
- **Akčný plán pre kybernetickú bezpečnosť** - tento akčný plán bude obsahovať konkrétne opatrenia, ktoré EÚ plánuje prijať na posilnenie kybernetickej bezpečnosti.

1.3 Smernica Európskeho parlamentu a rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2)

Základným a najobsiahlejším dokumentom riešiacim kybernetickú bezpečnosť je Smernica 2022/2555 (ďalej NIS2), ktorá nahradila pôvodnú smernicu 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Dôvodom na vypracovanie novej smernice bol nielen pokrok v oblasti info-komunikačných technológií (ďalej IKT) a rozvoj sietí a informačných systémov, ale predovšetkým riešenie viacerých problémov s jej rozdielnym výkladom a praktickým uplatňovaním zo strany jednotlivých členských štátov.

Nová smernica NIS2 rozširuje rozsah uplatňovania na väčšiu časť hospodárstva, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. Rovnako novo definuje orgány dohľadu a nimi uplatňované právomoci a procesy v oblasti kybernetickej bezpečnosti na národnej a medzinárodnej úrovni, ako aj rozširuje a prehlbuje kompetencie Európskej agentúry pre bezpečnosť sietí a informácií (ďalej ENISA).

1.3.1 Rozsah pôsobnosti

Smernica NIS2 jasne definuje organizácie spadajúce do jej pôsobnosti. Jedná sa o súkromné alebo verejné organizácie z odvetví s vysokou úrovňou kritickosti pre národné hospodárstvo alebo hospodárstvo EÚ, ktoré zároveň dosahujú alebo prekračujú limity pre zaradenie medzi stredné podniky[2] (zamestnávajú do 250 osôb a ročný obrat alebo celková bilančná suma nepresahuje 50 miliónov EUR). Za dôležitý subjekt je považovaný aj taký, ktorý členský štát EÚ označí za jediného poskytovateľa služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností.

V odvetví **Energetiky** sú to podniky spadajúce do nasledujúcich pododvetví:

- **Elektrická energia** - ide o elektroenergetické podniky vykonávajúce funkcie dodávky energie; prevádzkovateľov distribučných sústav; prevádzkovateľov prenosových sústav; výrobcov elektrickej energie; nominovaných organizátorov trhu s elektrickou energiou; účastníkov trhu poskytujúcich služby agregácie, riadenia odberu alebo uskladňovania energie; a prevádzkovateľov nabíjacieho bodu zodpovedných za prevádzku nabíjacieho bodu pre koncových užívateľov (a to aj v mene a na účet poskytovateľa služieb mobility).
- **Diaľkové vykurovanie a chladenie** - ide o prevádzkovateľov diaľkového vykurovania alebo diaľkového chladenia.
- **Ropa** - ide o prevádzkovateľov ropovodov; prevádzkovateľov zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu; a ústredné subjekty správy zásob.
- **Plyn** - ide o dodávateľské podniky; prevádzkovateľov distribučnej siete; prevádzkovateľov prepravnej siete, prevádzkovateľov zásobníkov, prevádzkovateľov zariadení LNG, plynárenské podniky[3]; a prevádzkovateľov zariadení na rafinovanie a spracovanie zemného plynu.
- **Vodík** - ide o prevádzkovateľov zariadení na výrobu, skladovanie a prepravu vodíka.

[2] Článok 2 prílohy k odporúčaniu 2003/361/ES
[3] Článok 2, bod 1 smernice 2009/73/ES

V odvetví **Dopravy** sú to podniky spadajúce do nasledujúcich pododvetví:

- **Letecká doprava** - ide o leteckých dopravcov; riadiace orgány letiska, letiská vrátane hlavných letísk a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách; ako aj prevádzkovateľov kontroly riadenia dopravy poskytujúcich služby riadenia letovej prevádzky (ATC).
- **Železničná doprava** - ide o manažérov infraštruktúry; a železničné podniky vrátane prevádzkovateľov servisných zariadení.
- **Vodná doprava** - ide o spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú, riadiace orgány prístavov vrátane ich prístavných zariadení a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu; ako aj prevádzkovateľov plavebno-prevádzkových služieb (VTS).
- **Cestná doprava** - ide o cestné orgány zodpovedné za kontrolu riadenia dopravy, s výnimkou verejných subjektov, v prípade ktorých je riadenie dopravy alebo prevádzkovanie inteligentných dopravných systémov nepodstatnou súčasťou ich celkovej činnosti; a prevádzkovateľov inteligentných dopravných systémov.

V odvetví **Bankovníctva** ide o úverové inštitúcie.[4]

V odvetví **Infraštruktúry finančných trhov** ide o centrálne protistrany (CCP).[5]

V odvetví **Zdravotníctva** ide o poskytovateľov zdravotnej starostlivosti; referenčné laboratóriá EÚ; subjekty vykonávajúce činnosti vo výskume a vývoji liekov; subjekty vyrábajúce základné farmaceutické výrobky a farmaceutické prípravky[6]; subjekty vyrábajúce zdravotnícke pomôcky považované za kritické v núdzovej situácii v oblasti verejného zdravia.

V odvetví **Pitnej vody** ide o dodávateľov a distribútorov vody určenej na ľudskú spotrebu, s výnimkou distribútorov, pre ktorých je distribúcia vody určenej na ľudskú spotrebu nepodstatnou súčasťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru.

V odvetví **Odpadovej vody** ide o podniky zaoberajúce sa zberom, likvidáciou alebo úpravou komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd s výnimkou podnikov, pre ktoré je zber, likvidácia alebo úprava komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd nepodstatnou súčasťou ich celkovej činnosti

V odvetví **Digitálnej infraštruktúry** ide o poskytovateľov internetových prepojovacích uzlov; poskytovateľov služieb systému názvov domén, s výnimkou prevádzkovateľov koreňových názvových serverov; správcov názvov domén najvyššej úrovne; poskytovateľov služieb cloud computingu; poskytovateľov služieb dátového centra; poskytovateľov sietí na sprístupňovanie obsahu; poskytovateľov dôveryhodných služieb (elektronických podpisov, elektronických pečatí, elektronických časových pečiatok, elektronických doručovacích služieb pre registrované zásielky a certifikátov pre autentifikáciu webových sídiel); poskytovateľov verejných elektronických komunikačných sietí; poskytovateľov verejne dostupných elektronických komunikačných služieb.

V odvetví **Riadenia** služieb **IKT** (medzi podnikmi) ide o poskytovateľov riadených služieb a riadených bezpečnostných služieb.

[4] Článok 4, bod 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013
[5] Článok 2, bod 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012
[6] Sekcia C divízie 21 NACE Rev.2

V odvetví týkajúcom sa **Vesmíru** ide o prevádzkovateľov pozemnej infraštruktúry, ktorú vlastnia, riadia a prevádzkujú členské štáty alebo súkromné subjekty, ktoré prispievajú k poskytovaniu vesmírnych služieb, s výnimkou poskytovateľov verejných elektronických komunikačných sietí.

V odvetví **Poštových služieb** ide o poskytovateľov poštových služieb, vrátane poskytovateľov kuriérskych služieb. Poskytovatelia poštových služieb, vrátane poskytovateľov kuriérskych služieb by mali podliehať tejto smernici, ak zabezpečujú aspoň jeden z krokov v reťazci poštového doručovania, a to najmä vyberanie, triedenie, prepravu alebo distribúciu poštových zásielok vrátane služieb zberu, pričom treba zohľadniť stupeň ich závislosti od sietí a informačných systémov. Dopravné služby, ktoré sa nevykonávajú v spojení s jedným z týchto krokov, by mali byť vyňaté z rozsahu poštových služieb.

V odvetví **Odpadového hospodárstva** ide o podniky vykonávajúce činnosti nakladania s odpadom, s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť.

V odvetví **Výroby a distribúcie chemických látok** ide o podniky vyrábajúce chemické látky a distribuujúce chemické látky alebo zmesi a podniky vyrábajúce výrobky z chemických látok a zmesí.[7]

V odvetví **Výroby, spracovania a distribúcie potravín** ide o potravinárske podniky, ktoré sa zaoberajú veľkoobchodnou distribúciou a priemyselnou výrobou a spracovaním.

V odvetví Výroby sú to podniky spadajúce do nasledujúcich pododvetví:

- **Výroba zdravotníckych pomôcok a diagnostických zdravotníckych pomôcok in vitro** - ide o subjekty vyrábajúce zdravotnícke pomôcky a diagnostické zdravotnícke pomôcky in vitro.
- **Výroba počítačových, elektronických a optických výrobkov** - ide o subjekty vykonávajúce akúkoľvek hospodársku činnosť v tejto oblasti.[8]
- **Výroba elektrických zariadení** - ide o subjekty vykonávajúce akúkoľvek hospodársku činnosť v tejto oblasti.[9]
- **Výroba iných nešpecifikovaných strojov a zariadení** - ide o subjekty vykonávajúce akúkoľvek hospodársku činnosť v tejto oblasti.[10]
- **Výroba motorových vozidiel, návesov a prívesov** - ide o subjekty vykonávajúce akúkoľvek hospodársku činnosť v tejto oblasti.[11]
- **Výroba ostatných dopravných prostriedkov** - ide o subjekty vykonávajúce akúkoľvek hospodársku činnosť v tejto oblasti.[12]

V odvetví **Poskytovateľov digitálnych služieb** ide o poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete.

V odvetví **Výskumu** ide o výskumné organizácie.

[7] Článok 3, body 3, 9 a 14 nariadenia Európskeho parlamentu a Rady (ES) č. 1907/2006
[8] Sekcia C divízie 26 NACE Rev. 2
[9] Sekcia C divízie 27 NACE Rev. 2
[10] Sekcia C divízie 28 NACE Rev. 2
[11] Sekcia C divízie 29 NACE Rev. 2
[12] Sekcia C divízie 30 NACE Rev. 2

1.3.2 Výnimky z rozsahu pôsobnosti

V prípade poskytovateľov verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb; poskytovateľov dôveryhodných služieb; registrátorov názvov domén najvyššej úrovne a poskytovateľov služieb systému názvov domén **je nutné upozorniť, že smernica NIS2 sa na nich vzťahuje bez ohľadu na veľkosť ich organizácie**.

Členské štáty EÚ majú takisto stanoviť, ktoré **mikropodniky** (do 10 zamestnancov s obratom alebo celkovou ročnou bilančnou sumou do 2 miliónov EUR) a **malé podniky** (do 50 zamestnancov s obratom alebo celkovou ročnou bilančnou sumou do 10 miliónov EUR) **spĺňajú kľúčovú úlohu pre spoločnosť, hospodárstvo alebo pre určité odvetvia, či druhy služieb. Takéto mikropodniky a malé podniky budú rovnako zaradené do pôsobnosti smernice NIS2**. Kritériá a usmernenia pre mikropodniky a malé podniky spadajúce do pôsobnosti smernice NIS2 vypracuje Európska komisia.

Samostatnou kapitolou sú organizácie verejnej správy. Z pohľadu MSP sa problematika smernice NIS2 vo vzťahu k verejnej správe stáva dôležitou v dvoch špecifických prípadoch:

Členské štáty môžu ustanoviť, že smernica **sa vťahuje** aj na vzdelávacie inštitúcie, najmä v prípade ak vykonávajú kritické výskumné činnosti. V takom prípade sa týka nielen verejných, ale **aj súkromných vzdelávacích pracovísk**. Vzhľadom na to, že fyzické a právnické osoby, ktoré skúmajú zraniteľnosti, by v niektorých členských štátoch mohli byť vystavené trestnej a občianskoprávnej zodpovednosti, členské štáty sa nabádajú, aby prijali usmernenia tykajúce sa nestíhania výskumníkov v oblasti bezpečnosti informácií a udelia tak výnimky z občianskoprávnej zodpovednosti za ich činnosť.

Smernica NIS2 sa naopak neuplatňuje v prípadoch, kedy je jej nadradená legislatíva členského štátu EÚ v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, odhaľovania a stíhania trestných činov. Hoci sa teda táto smernica vzťahuje aj na subjekty vykonávajúce činnosti v oblasti výroby elektrickej energie v jadrových elektrárňach, **niektoré z uvedených činností** výrobcu alebo dodávateľa **môžu súvisieť s národnou bezpečnosťou**. **V takom prípade sa smernica NIS2 na subjekt nevzťahuje a subjekt je povinný postupovať v rámci zodpovedajúcich ustanovení národnej legislatívy. Rovnako tak môže štát z pôsobnosti smernice NIS2 vyňať podnikateľský subjekt, ktorý poskytuje služby len subjektu verejnej správy pôsobiacom v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, odhaľovania a stíhania trestných činov.**

Malé a stredné podniky, ktoré neposkytujú kritické služby a nespadajú teda do pôsobnosti tejto smernice by zo strany štátu, dohliadajúcich orgánov, ako aj profesijných a stavovských združení mali byť podporované v dosahovaní takej úrovne kybernetickej bezpečnosti, ktorá bude odrážať ich maximálne možnosti riadenia kybernetických rizík. Ideálne by mali zaviesť rovnocenné opatrenia, aké sú predpísané subjektom spadajúcim do pôsobnosti smernice NIS2.

1.3.3 Dôležité, kľúčové a iné subjekty

Všetky subjekty, na ktoré sa smernica NIS2 vzťahuje, budú rozdelené podľa miery kritickosti pre štátnu (európsku) ekonomiku, ako aj podľa ich veľkosti. V nadväznosti na to budú zaradené do jednej z dvoch kategórií – buď ako **dôležité** alebo ako **kľúčové**. Na základe zaradenia bude k danému subjektu pristupované v rozsahu dohľadu, ako aj v rozsahu presadzovania práva.

Oficiálna definícia kľúčových a dôležitých podnikov zatiaľ chýba a nie je v uvedená ani v článku 6 nariadenia NIS2, ktorý vymedzuje základné pojmy. Za kľúčové sú však bežne považované tie, ktoré sú **kriticky dôležité** pre ekonomiku, zamestnanosť alebo pre zabezpečenie základných produktov a služieb, potrebných pre život. Dôležité podniky sú definované širšie. Patria medzi ne tie, ktoré sú **dôležité** pre ekonomiku, zamestnanosť, inovačný potenciál alebo pre zabezpečenie dôležitých produktov a služieb.

Každý členský štát EÚ je povinný vypracovať zoznamy dôležitých a kľúčových subjektov k **17. aprílu 2025**. Nemusí však byť povinnosťou štátu aktívne vyhľadávať subjekty, ktoré na tento zoznam zaradí. Túto povinnosť smie previesť na **samotné subjekty formou tzv. samoidentifikácie**, avšak za podmienky, že poskytne verejne dostupné informácie, metodiku, podporu a priestor pre ich samoidentifikáciu.

Všetky kritické subjekty musia dohliadajúcim orgánom predložiť, resp. sprístupniť údaje v minimálnom požadovanom rozsahu, a to:

- názov,
- adresu,
- aktuálne kontaktné údaje (vrátane e-mailových adries a telefónnych čísel),
- rozsahy IP adries,

Podľa potreby musia poskytnúť aj informácie o:

- zaradení do odvetvia, resp. pododvetvia,
- zozname členských štátov, v ktorých poskytujú služby patriace do pôsobnosti tejto smernice.

Rovnako ako v prípade samoidentifikácie, aj zodpovednosť za zaisťovanie bezpečnosti IKT je vo veľkej miere zodpovednosťou kľúčových a dôležitých subjektov. Tieto opatrenia by však mali zohľadňovať stupeň závislosti kľúčového alebo dôležitého subjektu od sietí a informačných systémov a mali by obsahovať **opatrenia na identifikáciu rizika incidentov**, opatrenia na **predchádzanie incidentom, ich odhaľovanie, reakciu na ne a zotavenie sa z nich**, ako aj opatrenia na **zmiernenie ich vplyvu**. Opatrenia by mali zároveň zohľadňovať najnovší technický vývoj v tejto oblasti, najaktuálnejšie európske a medzinárodné normy, ako aj náklady na ich vykonávanie. Bezpečnosť sietí a informačných systémov by mala zahŕňať **bezpečnosť uchovávaných, prenášaných a spracúvaných údajov**. Opatrenia na riadenie kybernetických rizík by mali zabezpečovať systémovú analýzu, pri ktorej sa zohľadní ľudský faktor, s cieľom získať úplný obraz o bezpečnosti siete a informačného systému. Cieľom by takisto malo byť, aby sa subjekty vyhli neprimeranému finančnému a administratívnemu zaťaženiu. Preto by opatrenia na riadenie kybernetických rizík mali byť primerané rizikám, ktorým čelí daná sieť a daný informačný systém, ako aj spoločenskému a hospodárskemu vplyvu, ktorý by incident mal.

Všetky kľúčové a dôležité subjekty by rámci smernice NIS2 mali zaistiť aj **bezpečnosť súkromných sietí**, do ktorých majú obvykle (vzdialený) prístup zamestnanci organizácie alebo iné osoby s patričným oprávnením. Za bezpečnosť takýchto intranetových sietí **zodpovedá kľúčový alebo dôležitý subjekt** tak v prípade, ak ich spravujú interní IT pracovníci, ako aj v prípade, ak je bezpečnosť zaisťovaná externe.

Európska komisia poskytne členským štátom (a sprostredkovane aj subjektom) usmernenia v prípade, ak má subjekt tak komplexný obchodný alebo organizačný model, že časť jeho aktivít spadá pod dôležité a časť pod kritické činnosti. Usmernenie poskytne aj v prípade, keď časť činností, ktoré vykonáva spadá pod pôsobnosť smernice NIS2 a časť je z jej pôsobnosti vyňatá.

V prípade kritických subjektov, ktoré vystupujú ako **partnerské podniky** alebo sú akokoľvek prepojené s inými podnikmi bude prihliadané na mieru ich prepojenia a závislosti vo vzťahu k ich zahraničným partnerom alebo organizačným jednotkám. Ak takýto subjekt preukáže nezávislosť svojich sietí a informačných systémov používaných pri poskytovaní svojich služieb od sietí a informačných systémov zahraničných partnerov, jeho zaradenie medzi stredné podniky sa môže javiť ako neprimerané. V takomto prípade môžu dohliadajúce orgány členského štátu rozhodnúť o vyradení takéhoto subjektu zo zoznamu stredných podnikov. Je však dôležité pripomenúť, že takýto krok automaticky nemusí zbavovať dotknutý subjekt povinnosti riadiť sa nariadením NIS2, obzvlášť ak poskytuje kritické služby. Rovnako ho nezbavuje povinností, ktorými sa podľa smernice NIS2 musia riadiť partnerské alebo inak prepojené podniky, ktoré spadajú do jej pôsobnosti.

Subjekty, ktorých podnikateľský model má **výrazný cezhraničný charakter** majú podliehať vysokej miere harmonizácie na úrovni EÚ. Z tohto dôvodu bude na riadenie kybernetických rizík vydaný zvláštny vykonávací akt pre nasledujúce typy subjektov:

- poskytovatelia služieb názvov domén, správcovia názvov domén najvyššej úrovne,
- poskytovatelia služieb cloud computingu, poskytovatelia služieb dátového centra,
- poskytovatelia sietí na sprístupňovanie obsahu, poskytovatelia riadených služieb,
- poskytovatelia riadených bezpečnostných služieb, poskytovatelia online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovatelia dôveryhodných služieb.

1.3.4 Kybernetické hrozby

V súčasnosti (2025) sú z pohľadu subjektov MSP najzávažnejšie štyri typy kybernetických útokov: útoky na dodávateľský reťazec, cloudové útoky, ransomvérové útoky a rozsiahle kyberincidenty (pôvodcom sú väčšinou iné štátne subjekty alebo ich proxy-subjekty), ktorých cieľom je znefunkčniť kritické siete, často súbežne vo viacerých štátoch EÚ.

Útoky na dodávateľský reťazec sú typom kybernetického útoku, pri ktorom sa útočníci zameriavajú na organizácie v dodávateľskom reťazci cieľovej obete. To znamená, že namiesto priameho útoku na cieľový subjekt alebo osobu sa útočníci snažia infiltrovať jej dodávateľov, partnerov alebo iné organizácie, ktoré sú s ňou prepojené. Cieľom týchto útokov môže byť krádež dát, inštalácia škodlivého softvéru, narušenie prevádzky alebo získanie prístupu k citlivým informáciám. Útoky na dodávateľský reťazec sú často sofistikované a môžu byť ťažko odhaliteľné, pretože si vyžadujú znalosť štruktúry a fungovania dodávateľského reťazca.

Podobným typom hrozby je útok na cloudové úložiská. Útočník sa obvykle snažiť získať prístup k dátam uloženým na cloudových úložiskách alebo narušiť prevádzku cloudových služieb.

Z hľadiska hrozieb je nutné zvýšenú pozornosť venovať aj **ransomvérovým útokom**, kde malvér šifruje údaje alebo systémy a požaduje od zasiahnutého subjektu platby za ich znovu sprístupnenie. Masívny nárast frekvencie a rozsahu takých útokov z posledných rokov súvisí s nárastom kriminálnych aktivít ako „podnikateľskej činnosti“, ako aj s rozvojom ťažko kontrolovateľného, paralelného komoditného systému kryptomien.

Najzávažnejšou formou kybernetických rizík sú **rozsiahle kyberincidenty**. Tieto sú definované ako incidenty schopné spôsobiť narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať, alebo ktoré majú významný vplyv aspoň na dva členské štáty EÚ. Rozsiahle kybernetické incidenty v závislosti od svojej príčiny a dosahu majú potenciál narušiť a poškodiť kritické informačné infraštruktúry. Môžu vystupňovať a naplno prepuknúť v krízu, ktorá neumožňuje riadne fungovanie vnútorného trhu alebo predstavuje vážne riziká

pre verejnú bezpečnosť a ochranu subjektov či občanov v niekoľkých členských štátoch alebo v celej EÚ.

Zabúdať nemožno ani na staršie typy hrozieb ako sú phishing, pokusy inštalovať do koncového zariadenia obete malvér alebo realizácia útokov s využitím sociálneho inžinierstva.

- **Phishing** - útočník sa snaží získať citlivé informácie (napr. prístupové heslá) prostredníctvom podvodných e-mailov alebo webových stránok. Phishing ostáva jednou z najčastejších metód kybernetických útokov.
- **Malvér** - útočník sa pokúša, obvykle prostredníctvom elektronickej pošty alebo textovej správy šíriť odkaz priamo na škodlivý softvér, ktorý môže poškodiť počítač alebo ukradnúť dáta. Malvér zahŕňa vírusy, trójske kone, spyware a adware.
- **Sociálne inžinierstvo** - útočník prostredníctvom psychologickej manipulácie obete získava citlivé informácie, prístup k financiám zasiahnutého subjektu alebo k jeho informačnému systému. Sociálne inžinierstvo sa obvykle využíva v kombinácii s inými typmi útokov.

Na opačnom spektre rizík sú nastupujúce kybernetické hrozby, ako útoky prostredníctvom krádeže digitálnej identity osôb alebo útoky s využitím umelej inteligencie, resp. tzv. internetu vecí. Nariadenia komplexne pokrývajúce tieto typy hrozieb sú v EÚ momentálne v príprave.

1.3.5 Kybernetická bezpečnosť

Členské štáty EU majú právo zriadiť jeden alebo viacero orgánov, zodpovedajúcich za kybernetickú bezpečnosť a úlohy dohľadu podľa smernice NIS2. Rovnako má každý členský štát možnosť zahrnúť časti nariadenia NIS2 do viacerých legislatívnych nástrojov. Členské štáty môžu od kľúčových a dôležitých subjektov vyžadovať, aby používali konkrétne produkty, služby a procesy IKT, ktoré vyvinul kľúčový alebo dôležitý subjekt alebo boli obstarané od tretích strán certifikovaných podľa európskych systémov certifikácie kybernetickej bezpečnosti.

U kľúčových alebo dôležitých subjektov, ktorým sú venované **samostatné odvetvové akty** sa z dôvodu vylúčenia nezrovnalostí alebo duplicity postupuje podľa predmetného odvetvového aktu[13], ktorý nadobúda rovnocenný účinok, ako smernica NIS2. V praxi to znamená, že kybernetická ochrana, ako aj nahlasovanie kybernetických incidentov musí byť aj v takomto prípade realizované minimálne na úrovni, akú garantuje nariadenie NIS2.

Monitorovanie a detekciu incidentov, ich analyzovanie, ako aj reakcie na incidenty a ich prevenciu by mala mať na starosti národná jednotka pre riešenie kybernetických incidentov (ďalej CSIRT). Jej zriadenie je v gescii každého členského štátu EÚ. Strešnou koordinačnou organizáciou národných jednotiek všetkých členských štátov EÚ a agentúrou ENISA je od roku 2020 Európska sieť styčných organizácií pre kybernetické krízy (ďalej EU-CyCLONe), ktorá zároveň funguje vo vzťahu k Európskej komisií ako sprostredkovateľ medzi technickou a politickou úrovňou riešenia kríz.

Jednotky CSIRT majú právo po žiadosti zo strany kritického subjektu **začať monitorovať aktivity subjektu** orientované na internet. A to ako **v jeho priestoroch**, tak aj mimo nich s cieľom identifikovať, pochopiť a riadiť organizačné riziká, a/alebo kritické zraniteľnosti subjektu. Subjekt tiež bude v takomto prípade požiadaný zo strany jednotky CSIRT o

[13] Takýmto významným odvetvovým aktom je napr. Nariadenie Európskeho parlamentu a rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA), vzťahujúce sa špecificky na kybernetickú bezpečnosť finančných inštitúcií.

poskytnutie informácie, či prevádzkuje privilegované rozhranie (časť systému prístupná len pre administrátorov), vzhľadom k tomu, že môže ovplyvniť rýchlosť vykonávaných opatrení.

V odôvodnených prípadoch majú národné jednotky CSIRT alebo európska agentúra ENISA, právo vykonať bezpečnostné audity alebo penetračné testovanie. Ako reakciu na prebiehajúci incident, s cieľom odvrátiť alebo zastaviť ho, majú obe jednotky (alebo iné poverené orgány podľa národnej legislatívy) právo vyslať za týmto účelom svojich odborníkov do priestorov zasiahnutého subjektu.

Pre nahlasovanie kybernetických incidentov, riešenie problémov, komunikáciu medzi jednotlivými subjektmi na národnej aj medzinárodnej úrovni je potrebné, aby každý členský štát zriadil aj **jednotné kontaktné miesto**.

Z dôvodu výmeny informácií medzi všetkými subjektmi zapojenými do riešenia kybernetických incidentov sa majú štátne orgány snažiť zharmonizovať vzorové formuláre na nahlasovanie incidentov, ak aj postupy dohľadu. V prípade, ak kritický subjekt nahlási kybernetický incident, **príslušné orgány** členského štátu **majú právo vymieňať si informácie s partnerskými orgánmi iného členského štátu** (resp. s celoeurópskymi inštitúciami ako sú agentúra ENISA alebo Europol) bez zbytočného odkladu, najmä ohľadom identifikácie kritického subjektu, kybernetických aj nekybernetických hrozbách a incidentoch, ktorým čelí, kybernetických a fyzických opatreniach, ktoré subjekt prijal aby im zamedzil, ako aj výsledkoch dohľadu vo vzťahu k takémuto subjektu. Cieľom výmeny informácií je mimo iné zabrániť vzniku kaskádového efektu šírenia kybernetickej hrozby, a to nielen z jedného členského štátu do ďalších, ale aj z menšieho subjektu na väčší.

Jednotky CSIRT vyšetrujúce kybernetické incidenty sa v priebehu šetrenia môžu dostať do kontaktu s **citlivými údajmi** osobného aj obchodného charakteru. Členský štát musí v tejto súvislosti zabezpečiť, aby personál jednotiek CSIRT bol dôveryhodný a proces nakladania s informáciami zachovával ich dôvernosť.

U podnikateľských subjektov z odvetvia digitálnej infraštruktúry (založených na sieťach a informačných systémoch, vrátane všetkých foriem cloudových úložísk), je nutné zabezpečiť v rámci kybernetickej bezpečnosti aj **fyzickú bezpečnosť úložísk**, dátových centier alebo iných zdrojov údajov. Toto opatrenie sa týka aj správcov domén najvyššej úrovne (top-level domain - TLD), tak aby bola prostredníctvom bezpečného systému názvov domén zabezpečená integrita internetu.

Subjekty, ktoré vyvíjajú alebo spravujú siete a informačné systémy, by mali zaviesť vhodné postupy na riešenie zistených zraniteľností. Keďže zraniteľností často odhaľujú a zverejňujú tretie strany, výrobca alebo poskytovateľ produktov alebo kľúčových a dôležitých služieb IKT by mal zaviesť aj potrebné postupy na prijímanie informácií o zraniteľnosti od tretích strán.[14] Koordinované zverejňovanie zraniteľností stanovuje štruktúrovaný proces, v rámci ktorého sa zraniteľnosti hlásia výrobcovi alebo poskytovateľovi potenciálne zraniteľných produktov alebo kľúčových služieb IKT takým spôsobom, ktorý mu umožňuje diagnostikovať a odstrániť zraniteľnosť pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú ďalším subjektom alebo verejnosti.

Pokiaľ ide o načasovanie nápravy a zverejnenie zraniteľnosti, koordinované poskytovanie informácií o zraniteľnosti by malo zahŕňať aj spoluprácu medzi oznamujúcou fyzickou alebo právnickou osobou a výrobcom alebo poskytovateľom potenciálne zraniteľných produktov, či služieb IKT. Členské štáty sú preto povinné poveriť jednu z národných jednotiek CSIRT ako koordinátora, ktorý bude pôsobiť ako dôveryhodný sprostredkovateľ medzi fyzickými a

[14] Pre usmernenie pozri medzinárodné normy ISO/IEC 30111 a ISO/IEC 29147.

právnickými osobami (aj v anonymnej pozícií) a výrobcami, resp. poskytovateľmi služieb alebo produktov IKT.

Členské štáty majú v súvislosti s kybernetickou bezpečnosťou za úlohu takisto podporovať využívanie inovatívnych technológií. V tejto súvislosti má byť kladený dôraz predovšetkým na nástroje umelej inteligencie, čo by mohlo zlepšiť a urýchliť proces prevencie a odhaľovania kybernetických útokov.

Z pohľadu malých a stredných podnikov je obzvlášť vhodné podporovať využitie **softvérových nástrojov s otvoreným zdrojovým kódom**. Ich aplikáciou sa proces zavádzania opatrení kybernetickej ochrany nielen zrýchli, ale umožní sa aj komunitný proces vyhľadávania a opráv zraniteľností systému. Hlavným prínosom pre MSP však je minimalizovanie potreby aplikácie špecifických nástrojov alebo aplikácií.

Súčasťou prijatých opatrení kybernetickej bezpečnosti by mali byť aj opatrenia aktívnej kybernetickej ochrany. Aktívna kybernetická ochrana je, na rozdiel od reaktívneho reagovania, aktívna prevencia, odhaľovanie, monitorovanie, analýza a zmierňovanie narušení bezpečnosti siete. Tieto aktívne opatrenia by sa zo strany štátu mali realizovať prostredníctvom bezplatných samoobslužných kontrol, detekčných nástrojov a služieb odstraňovania škodlivých softvérov. Aktívna kybernetická ochrana je však v každom ohľade obrannou stratégiou, ktorá vylučuje opatrenia akéhokoľvek ofenzívneho charakteru.

Predchádzaniu a riešeniu kybernetických incidentov by mala pomôcť aj celoeurópska databáza zraniteľností. Všetky subjekty, vrátane tých ktoré nepatria do pôsobnosti smernice NIS2, ich dodávatelia sietí a informačných systémov, ako aj jednotky CSIRT, by do tohto registra mohli (na báze dobrovoľnosti) zanášať zraniteľnosti, tak aby iným subjektom pomohli prijať vhodné opatrenia na elimináciu rizík. S cieľom podporiť kultúru zverejňovania zraniteľností by zverejnenie nemalo spôsobiť žiadnu ujmu oznamujúcej fyzickej alebo právnickej osobe.

Údaje zanášané do databázy zraniteľnosti by poľa článku 12 bodu 2 Smernice mali konkrétne obsahovať:

- informácie s opisom zraniteľností,
- zasiahnuté produkty alebo služby IKT a závažnosť zraniteľností z hľadiska okolností, za ktorých ju možno zneužiť,
- dostupnosť súvisiacich záplat a v prípade absencie dostupných záplat usmernenia poskytnuté príslušnými orgánmi alebo jednotkami CSIRT určené používateľom zraniteľných produktov a služieb IKT o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností.

Takéto registre už v súčasnosti síce exitujú, ale ich hostiteľmi a správcami sú subjekty mimo EÚ. Interná európska databáza zraniteľností, spravovaná agentúrou ENISA zabezpečí nielen lepšiu transparentnosť v procese zverejňovania pred tým, ako je konkrétna zraniteľnosť verejne oznámená, ale aj odolnosť v prípade prerušenia poskytovania podobnej služby. S cieľom podporiť kultúru zverejňovania zraniteľností by zverejnenie nemalo spôsobiť žiadnu ujmu oznamujúcej fyzickej alebo právnickej osobe. Aby sa však zabránilo zbytočnej duplicite pri zostavovaní registra, agentúra ENISA by mala preveriť možnosť uzatvorenia dohôd o zdieľaní (častí) obsahu podobných registrov, ktoré patria do právomocí mimoúnijných krajín.

V prípade potreby môže Európska komisia uzatvoriť medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorým môže povoliť (alebo organizovať ich účasť) **na vybraných činnostiach** skupiny pre spoluprácu, siete jednotiek CSIRT alebo siete EU-CyCLONe. Pri realizácií akejkoľvek spolupráce z mimioúnijnými subjektmi nesmie byť

dotknuté právo EÚ, ani vnútroštátne právo členského štátu EÚ v oblasti ochrany dôverných alebo utajovaných skutočností.

Keďže ohrozenie bezpečnosti sietí a informačných systémov môže mať rôzny pôvod, opatrenia na riadenie kybernetických rizík by sa mali zaoberať aj fyzickou a environmentálnou bezpečnostnou sietí a informačných systémov. Mali by tak obsahovať opatrenia na ochranu IKT pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi, ako sú napríklad krádež, požiar, povodeň, výpadok telekomunikačnej siete alebo elektrickej energie alebo pred neoprávneným fyzickým prístupom, poškodením alebo zásahom v súvislosti s informáciami kľúčového alebo dôležitého subjektu a jeho zariadeniami na spracovanie informácií. Všetky uvedené mimokybernetické hrozby by mohli ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracovávaných údajov alebo služieb, poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov. Všetky subjekty by preto mali prijať opatrenia na ochranu svojich softvérov a informačných systémov pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi. Rovnako by mali v rámci svojich opatrení na riadenie kybernetických rizík venovať zvýšenú pozornosť aj bezpečnosti ľudských zdrojov a mali by tak mať zavedené vhodné postupy kontroly prístupu.

Kľúčové a dôležité subjekty by sa rámci nariadenia NIS2 mali zameriavať aj na riešenie rizík vyplývajúcich zo vzťahov so spolupracujúcimi organizáciami. Mali by teda prijať súbor takých opatrení, ktoré budú chrániť obchodné tajomstvo a zabránia priemyselnej špionáži, a to principiálne u všetkých spolupracujúcich strán. Týka sa to predovšetkým kooperačných programov s akademickými a výskumnými inštitúciami. V súvislosti s podobnými pracoviskami je na základe nedávnych prípadov nutné aj citlivo a diskrétne preveriť, s akými ďalšími štátnymi a neštátnymi subjektmi partner z oblasti akademickej alebo výskumnej sféry spolupracuje. Minimalizuje sa tým riziko porušenia princípov ochrany duševného vlastníctva.

1.3.6 Dodávateľské reťazce, poskytovatelia dôveryhodných, interpersonálnych, komunikačných služieb a služieb registrácie domén

V oblasti kybernetických rizík, vo vzťahu k dodávateľskému reťazcu, sú kľúčové a dôležité subjekty nabádané posúdiť pôvod, kvalitu a odolnosť produktov a služieb, ako aj opatrenia a postupy dodávateľov produktov a služieb z radov vydavateľov softvérov, poskytovateľov riadených bezpečnostných služieb a poskytovateľov služieb ukladania a spracovania údajov. Zníži sa tým riziko zraniteľnosti týchto subjektov prostredníctvom využívania produktov a služieb dodaných treťou stranou. Súčasťou bezpečného pristupovania k dodávateľskému reťazcu je aj začlenenie opatrení na riadenie kybernetických rizík do zmluvných dohôd s dodávateľmi a poskytovateľmi softvérových produktov a služieb.

Zvláštnu pozornosť treba v tejto súvislosti venovať práve dodávateľom riadených bezpečnostných služieb (poskytujúcich služby ako napr. penetračné testovanie, bezpečnostné audity a poradenstvo). Tento typ poskytovateľov služieb sa môže stať sám cieľom kybernetického útoku, a preto ich hĺbkové zapojenie do činnosti subjektov môže predstavovať zvlášť vysoké riziko. Rizikový faktorom je aj vplyv tretej krajiny na dodávateľov a poskytovateľov produktov a služieb, najmä v prípade alternatívnych modelov riadenia. V produktoch alebo službách od takýchto poskytovateľov môžu byť skryté zraniteľnosti, zadné dvierka umožňujúce prístup do systému alebo môže hroziť potenciálne systémové narušenie dodávok alebo podpory. Platí to predovšetkým v situácii, keď je subjekt odkázaný na určitého dodávateľa technológie alebo je závislý od jediného poskytovateľa produktov alebo služieb.

Pre minimalizáciu kybernetických rizík kľúčového dodávateľského reťazca, Európska komisia a agentúra EINSA vypracujú pre každé odvetvie zoznam kritických služieb IKT, systémov a produktov IKT a relevantných hrozieb a zraniteľností. Takto komplexné posúdenie rizík umožní následne určiť opatrenia, plány zmierňovania a najlepšie postupy vo vzťahu ku kritickým závislostiam, potenciálnym jediným bodom zlyhania, hrozbám, zraniteľnostiam a ďalším rizikám spojeným s dodávateľským reťazcom. Pri rozhodnutiach, ktoré dodávateľské reťazce budú podliehať v jednotlivých odvetviach komplexnému posúdeniu bezpečnostných rizík sa bude prihliadať na:

- rozsah, v akom kľúčové a dôležité subjekty využívajú konkrétne kritické služby, systémy alebo produkty IKT a spoliehajú sa na ne,
- relevantnosť konkrétnych kritických služieb, systémov alebo produktov IKT pre vykonávanie kritických alebo citlivých funkcií vrátane spracúvania osobných údajov,
- odolnosť celkového dodávateľského reťazca služieb, systémov alebo produktov IKT počas ich životného cyklu voči rušivým udalostiam,
- v prípade vznikajúcich služieb, systémov alebo produktov IKT, na ich potenciálny budúci význam pre činnosti subjektov.
- zvláštna pozornosť bude venovaná službám, systémom alebo produktom IKT, ktoré pochádzajú z tretích krajín.

Povinnosti subjektov poskytujúcich dôveryhodné služby (ako napr. elektronický podpis, elektronická pečať, elektronická časová pečiatka, elektronické doručovacie služby, certifikáty pre autentifikáciu webových sídiel,...) aktuálne upravuje nariadenie (EÚ) č. 910/2014. Smernica NIS2 je pre tieto spoločnosti teda len doplňujúcim dokumentom, ukladajúca im povinnosť riadiť riziká ich služieb, a to aj vo vzťahu k zákazníkom a tretím stranám, spoliehajúcim sa na ich služby. Podľa smernice NIS2 sa subjekty poskytujúce dôveryhodné služby musia riadiť aj pri oznamovaní incidentov a pri princípoch fyzickej ochrany poskytovaných služieb. Naopak, požiadavky na kvalifikovaných poskytovateľov dôveryhodných služieb ostávajú zatiaľ tak, ako sú uvedené v nariadení č. 910/2014. Rovnako ostávajú podľa pôvodného nariadenia určené aj dohliadajúce orgány, ktoré sú však zaviazané spolupracovať s národnými jednotkami CSIRT, resp. obe strany dohliadajúcich orgánov si v prípade potreby majú poskytnúť vzájomnú súčinnosť.

V prípade subjektov poskytujúcich dôveryhodné služby je tak momentálne potrebné sa riadiť dvoma nariadeniami, pričom väčšinovo platí staršie nariadenie č. 91/2024. Keďže však ide o viac ako desať rokov starý dokument a technológie IKT, ako aj kybernetické hrozby sa odvtedy výrazne posunuli, očakáva sa, že pôvodné nariadenie bude obsahovo nahradené Európskym rámcom pre digitálnu identitu, resp. špecifickým odvetvovým aktom, ktorý z tohto dokumentu vzíde.

Nariadenie NIS2 sa okrajovo dotýka aj poskytovateľov interpersonálnych komunikačných služieb nezávislých od číslovania. Upozorňuje, že tento typ komunikačných kanálov (typicky napr. služby zasielania správ) sú častým vektorom útokov, najčastejšie prostredníctvom zasielania webových odkazov, ktoré obeť presmerujú na napadnuté internetové stránky. Poskytovatelia takýchto služieb by mali zaistiť bezpečnosť s ohľadom na podobné hrozby, avšak vzhľadom na to, že poskytovatelia interpersonálnych komunikačných služieb obvykle nemajú kontrolu nad prenosom signálu v sieti, miera rizika je v niektorých ohľadoch nižšia.

S cieľom zaistiť bezpečnosť verejných elektronických komunikačných sietí a verejne dostupných elektronických komunikačných služieb by sa malo podporovať používanie noriem bezpečného smerovania, ako aj používanie šifrovacích technológii, vrátane šifrovania bez

medzifáz. Okrem toho je vhodné uplatniť aj nasledujúce bezpečnostné koncepcie zamerané na údaje:

- **kartografia** - vytváranie máp dátových tokov a ich klasifikácia podľa dôležitosti a citlivosti.
- **segmentácia** - rozdelenie siete a dát do menších, izolovaných častí (segmentov), tak aby v prípade narušenia bezpečnosti došlo k obmedzeniu rozsah škôd a zabráneniu šírenia hrozby do celej siete.
- **označovanie** – dátam sú priraďované štítky, ktoré definujú ich vlastnosti, ako napríklad úroveň citlivosti, účel použitia alebo vlastníka, čo uľahčuje ich správu a kontrolu prístupu,
- **politika prístupu a riadenie prístupu** - definovanie pravidiel, kto má prístup k akým dátam a za akých podmienok,
- **automatizované rozhodnutia o prístupe** - využívanie automatických systémov na vyhodnocovanie žiadostí o prístup na základe definovaných pravidiel a kontextu, ako eliminácia ľudských chýb.

Nariadenie NIS2 kladie požiadavky aj na subjekty poskytujúce služby registrácie názvov domén. Podľa nariadenia sa od týchto subjektov bude požadovať spracovanie preddefinovaných údajov, za účelom vytvorenia databáz registračných údajov názvov domén (WHOIS). Vytvorenie takejto databázy je nutné na zaistenie bezpečnosti, stability a odolnosti systému názvov domén (DNS) ako aj pre napomáhanie zvládania kybernetických incidentov. Od subjektov poskytujúcich služby registrácie názvov domén a správcov registrov názvov domén sa vyžaduje, aby stanovili politiky a postupy zhromažďovania a uchovávania presných a úplných registračných údajov názvov domén, ako aj predchádzania nepresným registračným údajom a ich opravy. Takisto je potrebné zaviesť postupy na overovanie registračných údajov názvov domén, ako sú napríklad kontroly „ex ante“ v čase registrácie a kontroly „ex post“ vykonávané pravidelne po registrácií. V rámci procesu overovania by mala byť vždy overená aspoň jedna z možností funkčného kontaktu žiadateľa o registráciu.

V prípade registračných údajov názvov domén právnických osôb, ktoré nepatria do rozsahu pôsobnosti práva Únie v oblasti ochrany údajov, sa bude vyžadovať aspoň zverejnenie mena, resp. názvu žiadateľa, kontaktného telefónneho čísla a v prípade, ak neobsahuje osobné údaje, aj zverejnenie e-mailovej adresy. Sprístupnené by mali byť aj špecifické registračné údaje názvov domén fyzických osôb podľa európskeho práva v oblasti ochrany údajov.

Údaje majú byť bezplatne sprístupnené všetkým oprávneným žiadateľom, teda všetkým fyzickým a právnickým osobám, ktoré podali žiadosť podľa úniového alebo vnútroštátneho práva. Oprávneným žiadateľom sú aj dohliadajúce a vyšetrujúce orgány na národnej alebo európskej úrovni. Subjekty poskytujúce služby registrácie názvov domén a správcovia registrov názvov domén sú v tejto súvislosti povinní vypracovať politiky a postupy zverejňovania a sprístupňovania registračných údajov, vrátanie technického nástroja (rozhrania, portálu) na podávanie žiadostí o poskytnutie registračných údajov a prístupu k nim.

1.3.7 Manažment kybernetických rizík na úrovni podnikateľských subjektov

Riadiace orgány kľúčových a dôležitých subjektov sú povinné schváliť opatrenia na riadenie kybernetických rizík a prijať aj vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnostnou sietí a informačných systémov, ktoré využívajú na svoju činnosť alebo na poskytovanie svojich služieb.

Tieto opatrenia by podľa článku 21 bodu 2 Smernice mali zahŕňať najmenej:

- zásady analýzy rizík bezpečnosti informačných systémov,
- riešenie incidentov,
- kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii a krízové riadenie,
- bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov tykajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb,
- bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach,
- zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík,
- základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti,
- zásady a postupy používania kryptografie, pripadne šifrovania,
- bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív,
- v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.

Nariadenie NIS2 ukladá členským štátom EÚ povinnosť vypracovať aj politiky **kybernetickej hygieny**, zahŕňajúce základný súbor postupov, ktorými by sa dotknuté subjekty mali riadiť.

Patria medzi ne:

- používanie certifikovaných produktov, služieb a procesov IKT
- aktualizácie softvérov a hardvérov,
- zmeny hesiel,
- správy identít,
- informovanosť užívateľov,
- školenia pre zamestnancov,
- zásady nulovej dôvery,
- riadenia nových inštalácií,
- obmedzenia prístupových účtov na úrovni správcov,
- segmentácie sietí,
- zálohovanie údajov.

Členovia riadiacich orgánov kľúčových a dôležitých subjektov sú povinní absolvovať odbornú prípravu v oblasti kybernetických rizík a pravidelne zaistiť zamestnancom podobnú odbornú prípravu, aby títo nadobudli dostatočné znalosti a zručnosti a vedeli rozpoznať kybernetické riziká a ich vplyv na služby poskytované subjektom.

1.3.8 Priebeh a oznamovanie incidentov

Smernica NIS2 stanovuje viacfázový prístup k oznamovaniu kybernetických incidentov. Cieľom takéhoto prístupu je nájsť rovnováhu medzi rýchlym oznámením bezprostredne prebiehajúceho incidentu a spracovaním podrobnej správy, ktorej zverejnenie má iným subjektom poskytnúť dôležité informácie o charaktere hrozby a spôsobe vysporiadania sa s ňou. Dotknutým subjektom sa tiež odporúča, aby kybernetické hrozby nahlasovali dobrovoľne

a zabránili tak situáciám, kedy kybernetická hrozba prerastie do incidentu, ktorý spôsobí značnú materiálnu alebo nemateriálnu ujmu.

Prvotné posúdenie kybernetického incidentu je v kompetencií zasiahnutého subjektu, ktorý identifikuje hrozbu vážneho narušenia služieb, hrozbu vedúcu k potenciálnym finančným stratám alebo hrozbu, ktorá by iným fyzickým alebo právnickým osobám mohla spôsobiť majetkovú alebo nemajetkovú ujmu (vrátane podozrenia na únik osobných údajov alebo digitálnej identity). Pri prvotnom posúdení sa musia zvážiť dotknuté siete a informačné systémy, ich význam pri poskytovaní služieb subjektu, závažnosť a technické vlastnosti kybernetickej hrozby a všetky s ňou súvisiace zraniteľnosti. Ukazovatele ako rozsah a trvanie incidentu alebo počet zasiahnutých zákazníkov pomáhajú v zhodnotení miery závažnosti hrozby.

Kľúčové a dôležité subjekty sú podľa nariadenia NIS2 povinné bezprostredne, najneskôr však do 24 hodín po identifikácií kybernetického útoku vydať včasné varovanie. Včasné varovanie má obsahovať len tie informácie, ktoré sú potrebné pre oznámenie incidentu národnej jednotke CSIRT: podozrenie, či je incident spôsobený nezákonným konaním, zlým úmyslom, že incident súvisí so závažnou trestnou činnosťou a či môže mať cezhraničný dosah. Národná jednotka v prípade potreby tieto informácie odovzdá partnerským jednotkám v dotknutých krajinách a zasiahnutý subjekt sa tak môže sústrediť na riešenie incidentu.

Do 72 hodín po identifikácií kybernetického útoku musí napadnutý subjekt vydať oznámenie o incidente. Táto správa by mala aktualizovať informácie uvedené vo včasnom varovaní a poskytnúť prvotné hodnotenia incidentu, vrátane jeho závažnosti, vplyvov, prípadne (ak sú už známe) aj ukazovateľov narušenia.

Záverečnú správu by dotknutý subjekt mal odoslať do jedného mesiaca po identifikácií kybernetického útoku. Ak v tomto období kybernetický útok stále prebieha, dohliadajúce jednotky CSIRT dotknutých členských štátov sú povinné zabezpečiť, aby napadnuté subjekty poskytli priebežnú správu. Termín na odovzdanie záverečnej správy sa v takom prípade posúva na jeden mesiac odo dňa, kedy bol incident vyriešený.

V prípade ak sa podozrenie na kybernetickú hrozbu potvrdí, dotknutý subjekt je povinný informovať príjemcov svojich služieb o hrozbe, ako aj o opatreniach a prostriedkoch, ktoré na jej elimináciu a nápravu boli prijaté, zvlášť ak znamenajú obmedzenie služby. Tieto informácie musia byť poskytnuté bezplatne a musia byť formulované v ľahko zrozumiteľnom jazyku. Požiadavka na informovanie príjemcov služieb o kybernetickej hrozbe nezbavuje zasiahnutý subjekt primárnej povinnosti na túto hrozbu reagovať a v čo najkratšom čase obnoviť bežnú úroveň služby.

Pre zjednodušenie a zefektívnenie oznamovania informácií o kybernetickej hrozbe pre subjekty, ktoré sa nachádzajú v procese riešenia incidentov alebo odstraňujú ich následky, sú členské štáty povinné poskytnúť subjektom podporu a vhodné technické prostriedky. Tie by mali zahŕňať jednotné kontaktné miesto, automatizované systémy, online formuláre, ľahko použiteľné rozhrania, šablóny, prípadne špecializované platformy.

Predovšetkým existencia jednotného kontaktného miesta je dôležitá aj pre zníženie administratívnej záťaže zasiahnutých subjektov, ktoré by podľa tejto smernice, odvetvových aktov a národnej legislatívy museli inak často oznamovať informácie o incidente viacerým národným a európskym orgánom dohľadu a vyšetrovania. Po vyplnení štruktúrovaných formulárov o kybernetickom incidente a ich podaní na jednotnom kontaktnom mieste, toto v

zastúpení zasiahnutého subjektu zabezpečí aby sa informácie o incidente dostali ku všetkým relevantným orgánom dohľadu a vyšetrovania.

1.3.9 Dohľad nad subjektami a princípy teritoriality

Subjekty patriace do rozsahu pôsobnosti smernice NIS2 sa považujú za subjekty podliehajúce právomoci **členského štátu, v ktorom sú usadené**.

Ak subjekt poskytuje služby alebo je usadený vo viac ako jednom členskom štáte, mal by podliehať samostatnej a súbežnej právomoci každého z týchto členských štátov. **Poskytovatelia verejných elektronických komunikačných sietí** alebo **poskytovatelia verejne dostupných elektronických komunikačných služieb** by sa tak mali považovať za poskytovateľov podliehajúcich právomoci **každého členského štátu**, v ktorom poskytujú služby.

Poskytovatelia služieb názvov domén, správcovia názvov domén najvyššej úrovne (TLD), subjekty, ktoré poskytujú **služby registrácie názvov domén pre** TLD, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátových centier, poskytovatelia sietí na sprístupňovanie obsahu, poskytovatelia riadených služieb, poskytovatelia riadených bezpečnostných služieb, ako aj **poskytovatelia online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí** by mali byť považovaní za subjekty podliehajúce právomoci toho členského štátu, v ktorom majú **hlavnú prevádzkareň v Únii**. Právna forma takejto prevádzkarne, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou nie je určujúcim faktorom. Určujúcim faktorom takisto nie je fakt, či sa sieť a informačné systémy fyzicky nachádzajú na území Únie. Samotná prítomnosť a používanie takýchto systémov ako takých teda nepredstavuje hlavnú prevádzkareň. Za hlavnú prevádzkareň by sa mal považovať členský štát, kde sa najčastejšie prijímajú rozhodnutia o opatreniach na riadenie rizík kybernetickej bezpečnosti. Zvyčajne bude zodpovedať miestu ústredia subjektov v Únii. Ak takýto členský štát nemožno určiť alebo ak sa takéto rozhodnutia neprijímajú v Únii, za hlavnú prevádzkareň by sa mal považovať členský štát, v ktorom sa operácie kybernetickej bezpečnosti vykonávajú. Ak takýto členský štát nemožno určiť, za hlavnú prevádzkareň by sa mal považovať členský štát, v ktorom má subjekt prevádzkareň s najvyšším počtom zamestnancov v Únii. Ak služby vykonáva skupina podnikov, hlavná prevádzkareň riadiaceho podniku by sa mala považovať za hlavnú prevádzkareň skupiny podnikov.

V prípade typov **subjektov** uvedených v predchádzajúcom odstavci, **ktoré nie sú usadené v Únii**, ale na tomto trhu poskytujú alebo chcú poskytovať služby, sú tieto povinné **určiť** v EÚ **svojho zástupcu**. Zástupca má konať prostredníctvom písomného mandátu v mene subjektu, a to aj vo vzťahu k povinnostiam subjektu stanoveným v tejto smernici, vrátane oznamovania incidentov.

Smernica NIS2 stanovuje aj zoznam **opatrení a prostriedkov dohľadu**, prostredníctvom ktorých môžu príslušné orgány vykonávať dohľad nad kľúčovými a dôležitými subjektmi.

Miera dohľadových opatrení by pritom mala byť odlišná pre kľúčové a dôležité subjekty, zabezpečujúc tak spravodlivú rovnováhu ich povinností. Vykonávanie opatrení dohľadu musí byť realizované tak, aby minimalizovalo dopady na podnikateľskú činnosť preverovaného subjektu. V závažných prípadoch, kedy sa dohliadajúci orgán na základe svojho šetrenia rozhodne zabrániť hroziacemu kybernetickému incidentu, má právo prijímať na základe povahy hrozby adekvátne okamžité rozhodnutia, ktoré môžu viesť aj k obmedzeniu podnikateľskej činnosti subjektu.

Dôležité subjekty podliehajú len reaktívnemu **dohľadu „ex post“**. Tento typ subjektov teda nemusí systematicky dokumentovať súlad s opatreniami na riadenie rizík kybernetickej bezpečnosti. Dohlaď nad dôležitými subjektmi ex post môžu vyvolať dôkazy, indície alebo informácie, na ktoré boli príslušné orgány upozornené, a ktoré tieto orgány považujú za potenciálne porušenie tejto smernice. Dôkazy, indície alebo informácie môžu pochádzať od iných orgánov, subjektov, občanov, médií, z iných (verejne) dostupných zdrojov alebo môžu vyplynúť z iných činností, ktoré príslušné orgány vykonávajú pri plnení svojich úloh.

Dohľadové opatrenia pre dôležité subjekty zahŕňajú podľa článku 33 odsek 2 Smernice prinajmenšom:

- inšpekciu na mieste a „ex post“ dohlaď na diaľku, ktoré vykonávajú vyškolení odborníci,
- cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán alebo príslušný orgán,
- bezpečnostnú kontrolu založenú na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom,
- žiadosť o informácie potrebné na „ex post“ posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predkladať informácie príslušným orgánom podľa článku 27,
- žiadosť o prístup k údajom, dokumentom a informáciám potrebným na plnenie úloh dohľadu,
- žiadosť o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.

Kľúčové subjekty by mali podliehať komplexnému **dohľadu „ex post“ aj „ex ante“**. Pri dohľade „ex ante“ majú dohliadajúce orgány možnosť rozhodnúť o prednostnom použití opatrení a prostriedkov na základe ich internej metodiky. Obsahom takejto metodiky môžu byť napríklad kritériá alebo referenčné hodnoty na klasifikáciu kľúčových subjektov do kategórií rizík alebo frekvencie a typy inšpekcií.

Dohľadové opatrenia pre kľúčové subjekty zahŕňajú podľa článku 32 odseku 2 Smernice prinajmenšom:

- inšpekciu na mieste a dohlaď na diaľku, vrátane náhodných kontrol, ktoré vykonávajú vyškolení odborníci,
- pravidelný a cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán alebo príslušný orgán a hradí auditovaný subjekt,
- audit ad hoc, a to v prípadoch odôvodnených významným incidentom alebo porušením tejto smernice kľúčovým subjektom,
- bezpečnostnú kontrolu podľa objektívnych, nediskriminačných, spravodlivých a transparentných kritérií posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom,
- žiadosť o informácie potrebné na posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predložiť informácie príslušným orgánom podľa článku 27,
- žiadosť o prístup k údajom, dokumentom a informáciám potrebným na plnenie úloh dohľadu,

- žiadosť o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov, uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.

1.3.10 Sankcie

Za porušenie opatrení smernice NIS2 sa stanovuje minimálny rozsah právomocí presadzovania práva, uplatňovaný vo všetkých členských štátoch EÚ. Dohliadajúce orgány podľa článku 32 odseku 4 môžu:

- vydávať varovania o porušeniach tejto smernice dotknutými subjektmi,
- prijímať záväzné pokyny, a to aj v súvislosti s opatreniami potrebnými na prevenciu alebo nápravu incidentu, ako aj lehotami na vykonávanie takýchto opatrení a podávať správy o ich vykonávaní alebo príkazy, ktorými sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenia tejto smernice,
- nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu a takéto konanie neopakovali,
- nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zabezpečili zosúladenie svojich opatrení na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23,
- nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na túto hrozbu,
- nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania vydané na základe bezpečnostného auditu,
- určiť monitorujúceho úradníka s presne vymedzenými úlohami na určité obdobie, ktorý bude dohliadať u dotknutých subjektov na dodržiavanie článkov 21 a 23 dotknutými subjektmi,
- nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice,
- uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až h) tohto odseku.

Pri posudzovaní pochybenia by malo byť prihliadané k povahe, závažnosti a trvaniu porušenia tejto smernice, spôsobenej hmotnej a nehmotnej ujme nezávisle od toho, či bolo porušenie úmyselné alebo z nedbanlivosti, opatreniam prijatým na zabránenie alebo zmiernenie hmotnej alebo nehmotnej ujmy, miere zodpovednosti alebo predchádzajúcemu porušeniu nariadenia, miere spolupráce s príslušným orgánom a akýmkoľvek ďalším priťažujúcim alebo poľahčujúcim faktorom.

Pri presadzovaní práva by dohliadajúce orgány mali mať možnosť v prípade porušenia alebo ignorovania nariadení tejto smernice udeľovať finančné sankcie, vrátané pravidelných penále, ak porušovanie trvá v čase. Samotná smernica NIS2 ustanovuje výšku sankcií:

- pre kľúčové podniky - maximálne 10.000.000,- EUR alebo maximálne 2 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia a

- pre dôležité subjekty - maximálne 7.000.000,- EUR alebo maximálne 1,4 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia.

Oprávnenie udeľovať finančné sankcie, aj ich (prípadne nižšiu ako Úniou navrhnutú maximálnu) výšku však **ponecháva na jednotlivých členských štátoch** Únie. Tieto sú povinné zapracovať sankčný mechanizmus a maximálnu výšku sankcie v danej krajine do vnútroštátnej legislatívy.

Správna pokuta za porušenie alebo ignorovanie smernice NIS2 môže byť udelená kľúčovému alebo dôležitému subjektu, ktorým je podnik, rovnako ako je možné ju udeliť osobe, ktorá nie je podnikom. Ak je pokuta udeľovaná osobe, je pri rozhodovaní o primeranej výške pokuty nutné zohľadniť všeobecnú úroveň príjmov v členskom štáte, ako aj majetkové pomery danej osoby.

Smernica NIS2 sama o sebe nevyžaduje po členských štátoch aby vyvodzovali voči fyzickým osobám zodpovedným za zabezpečenie súladu subjektu s týmto nariadením trestnoprávnu alebo občianskoprávnu zodpovednosť, ak v súvislosti s porušením tejto smernice utrpeli škodu tretie strany. V prípade závažného porušenia tejto smernice tak rozhodnutie o tom, či udelené sankcie budú trestnoprávne alebo občianskoprávne, ostáva opäť výlučnou vecou vnútroštátnej právnej úpravy konkrétneho členského štátu Únie.

V prípadoch závažného alebo opakujúceho porušenia tejto smernice, má mať dohliadajúci orgán právomoc dočasne pozastaviť certifikácie alebo povolenia časti alebo všetkých relevantných služieb alebo činností, ktoré poskytuje kľúčový subjekt. Dohliadajúci orgán má mať v takýchto prípadoch možnosť požadovať pre fyzické osoby uloženie dočasného zákazu vykonávať riadiace funkcie na úrovni výkonného riaditeľa alebo právneho zástupcu. Tento typ sankcií však majú dohliadajúce organy udeľovať len v krajných prípadoch, po vyčerpaní ostatných sankčných opatrení a s prihliadnutím na okolnosti každého jednotlivého prípadu vrátane skutočnosti, či išlo o úmyselné alebo nedbanlivostné porušenie. Takisto je potrebné prihliadať aj na akékoľvek opatrenia, ktoré subjekt prijal na zabránenie alebo zmiernenie vzniknutej hmotnej či nehmotnej ujmy.

1.3.11 Špecifické výzvy pre malé a stredné podniky v kontexte smernice NIS2

Členské štáty by sa mali vo svojich národných stratégiách kybernetickej bezpečnosti zaoberať osobitnými potrebami, ktoré majú v oblasti kybernetickej bezpečnosti malé a stredné podniky. **Malé a stredné podniky** predstavujú v celej Únii veľký percentuálny podiel priemyselného a obchodného trhu a často majú **ťažkosti s prispôsobením sa novým obchodným postupom a digitálnemu prostrediu**, v ktorom zamestnanci pracujú z domu a obchodné činnosti sa čoraz častejšie vykonávajú online. Niektoré malé a stredné podniky čelia špecifickým problémom, ako sú **nízke kybernetické povedomie, nedostatočná bezpečnosť vzdialených IT, vysoké náklady na riešenia** v oblasti kybernetickej bezpečnosti a **zvýšená úroveň hrozieb**, ako je napríklad ransomvér, v súvislosti s ktorými by mali dostať usmernenia a podporu.

Malé a stredné podniky sa čoraz viac stávajú **terčom útokov na dodávateľské reťazce** z dôvodu ich menej prísnych opatrení na riadenie kybernetických rizík a zvládanie útokov ako aj skutočnosti, že majú obmedzené bezpečnostné zdroje. Takéto útoky na dodávateľské reťazce majú vplyv nielen na malé a stredné podniky a ich izolovanú činnosť, ale môžu mať aj kaskádový účinok na väčšie subjekty, ktorým poskytli dodávky.

Členské štáty by mali prostredníctvom svojich národných stratégií kybernetickej bezpečnosti pomáhať malým a stredným podnikom pri riešení výziev, ktorým čelia vo svojich dodávateľských reťazcoch. Mali by preto zriadiť kontaktné miesto pre MSP na národnej alebo regionálnej úrovni, ktoré buď poskytuje usmernenia alebo ich nasmeruje na príslušné orgány, ktoré im poskytnú v súvislosti s problematikou kybernetickej bezpečnosti usmernenia a pomoc. Členským štátom sa podľa nariadenia NIS2 tiež odporúča, aby mikropodnikom a malým podnikom, ktoré nemajú takéto kapacity, ponúkali služby ako sú konfigurácia a protokolovanie webových stránok.

1.4 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR)

Toto nariadenie sa vzťahuje na prevádzkovateľov databáz osobných údajov občanov a osôb usadených v EÚ alebo sprostredkovateľov, ktorí poskytujú prostriedky (softvér) na spracovávanie takto definovaných osobných údajov, a to bez rozdielu či sú tieto prostriedky používané na verejný, komerčný alebo súkromný účel. Pre uplatnenie tohto nariadenia nie je rozhodujúce, či prevádzkovateľ alebo sprostredkovateľ vykonáva spracovanie údajov na území Únie alebo mimo jej územia.

Zásady kybernetickej bezpečnosti, ako aj ochrana práv fyzických osôb pri spracúvaní osobných údajov si vyžaduje, aby sa prijali primerané technické a organizačné opatrenia s cieľom zabezpečiť ochranu osobných údajov tykajúcich sa identifikovanej alebo potenciálne identifikovateľnej fyzickej osoby.

Na to, aby mohol prevádzkovateľ preukázať súlad s týmto nariadením, mal by prijať interné pravidlá a opatrenia špecificky, resp. štandardne navrhnutej ochrany údajov.

Tieto opatrenia by mali okrem iného pozostávať zo spracovávania osobných údajov len v nevyhnutne minimálnej miere. Týka sa to množstva získaných osobných údajov, rozsahu ich spracúvania, doby ich uchovávania a ich dostupnosti. Na chránené spracovávanie a uchovávanie údajov sa majú využívať v aktuálnej dobe primerané dostupné technické a organizačné opatrenia. V súčasnosti je takým riešením napríklad pseudoanonymizácia údajov. Osobné údaje, ktoré boli pseudoanonymizované, ale mohli by sa použitím dodatočných informácií priradiť fyzickej osobe, by sa mali považovať za informácie o identifikovateľnej fyzickej osobe.

Ak pri získavaní a uchovávaní osobných údajov spolupracujú dvaja alebo viacerí prevádzkovatelia, sú považovaní za spoločného prevádzkovateľa. V takomto prípade sú si povinní formou dohody určiť príslušné zodpovednosti vo vzťahu k povinnostiam uvedeným v tomto nariadení. V zmluve uvedú nielen konkrétne rozdelenie svojich úloh, ale aj svoje vzťahy k osobám, ktorých osobné údaje spracovávajú. Dotknuté osoby však môžu bez ohľadu na podmienky dohody uplatniť svoje práva u ktoréhokoľvek subjektu spoločného prevádzkovateľa.

Prevádzkovateľ databázy osobných údajov, môže na ich získanie alebo spracovanie použiť sprostredkovateľa. Pri jeho výbere musí prihliadať na to, či sprostredkovateľ má alebo dokáže prijať dostatočné technické a organizačné opatrenia na ochranu osobných údajov dotknutých osôb. Sprostredkovateľ nesmie bez vedomia prevádzkovateľa databázy zapojiť do procesu nakladania s osobnými údajmi sekundárneho sprostredkovateľa (ak táto možnosť nie je súčasťou zmluvy). V prípade, že sprostredkovateľ chce do procesu spracovávania osobných údajov zapojiť sekundárneho sprostredkovateľa alebo už kooperujúceho nahradiť iným, je povinný o tejto skutočnosti neodkladne vyrozumieť prevádzkovateľa databázy. Na každého ďalšieho sprostredkovateľa sa automaticky vzťahujú ustanovenia tohto nariadenia. V prípade, ak ich sekundárny sprostredkovateľ poruší, voči prevádzkovateľovi databázy nesie zodpovednosť primárny sprostredkovateľ, s ktorým bola uzatvorená dohoda.

Spracúvanie sprostredkovateľom sa riadi zmluvou podľa práva Únie alebo práva členského štátu, ktoré zaväzuje sprostredkovateľa voči prevádzkovateľovi. V zmluve sa stanovuje predmet a doba spracovania, povaha a účel spracúvania, typ osobných údajov, kategórie

dotknutých osôb, ako aj povinnosti a práva prevádzkovateľa. Nariadenie v článku 28 vo vzťahu k podnikateľským subjektom uvádza, že zmluva sprostredkovateľovi stanovuje najmä:

- spracúvať osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo do nadnárodnej organizácie, s výnimkou prípadov, keď si to vyžaduje právo Únie alebo právo členského štátu, ktorému sprostredkovateľ podlieha - v takom prípade sprostredkovateľ oznámi prevádzkovateľovi túto právnu požiadavku pred spracovaním, pokiaľ dané právo takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu,
- zabezpečiť, aby sa osoby oprávnené spracovať osobné údaje zaviazali, že zachovajú dôvernosť informácií alebo aby boli viazané vhodnou povinnosťou zachovávať dôvernosť informácií vyplývajúcou zo štatútu,
- vykonať všetky opatrenia na zistenie bezpečnosti osobných údajov, a to konkrétne: pseudoanonymizáciu a šifrovanie osobných údajov, zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb, zabezpečiť schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu a zabezpečiť proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.
- dodržiavať vyššie uvedené podmienky zapojenia ďalšieho sprostredkovateľa,
- po zohľadnení povahy spracovania, v čo najväčšej miere pomáhať prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej fyzickej osoby,
- pomáhať prevádzkovateľovi zabezpečiť plnenie povinností, predovšetkým voči orgánom dozoru a dotknutej fyzickej osobe, s prihliadnutím na povahu spracúvania a informácie dostupné sprostredkovateľovi;
- po ukončení poskytovania služieb, tykajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa, všetky osobné údaje vymazať alebo vrátiť prevádzkovateľovi a vymazať existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov,
- poskytnúť prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia týchto povinností a umožniť so svojou aktívnou súčinnosťou audity, ako aj kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ.

Ak sprostredkovateľ preukáže dodržiavanie schváleného kódexu správania alebo schváleného certifikačného mechanizmu, prevádzkovateľ databázy to môže považovať za dostatočnú záruku bezpečného nakladania s osobnými údajmi.

1.4.1 Záznamy o spracovateľských činnostiach

Prevádzkovatelia databáz sú povinní viesť záznamy o spracovateľských činnostiach, za ktoré sú zodpovední, a to v písomnej podobe (aj v elektronickej forme). Tieto záznamy musia podľa článku 30 Nariadenia obsahovať nasledujúce informácie:

- meno/názov a kontaktné údaje prevádzkovateľa a v príslušnom prípade spoločného prevádzkovateľa, zástupcu prevádzkovateľa a zodpovednej osoby,
- účely spracúvania;
- opis kategórií dotknutých osôb a kategórií osobných údajov;
- kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, vrátane príjemcov v tretích krajinách alebo nadnárodných organizáciách,

- v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo do nadnárodnej organizácie, vrátane označenia predmetnej tretej krajiny alebo nadnárodnej organizácie a v prípade prenosov uvedených v článku 49 os. 1 druhom pododseku dokumentáciu primeraných záruk,
- podľa možností predpokladané lehoty na vymazanie rôznych kategórií údajov,
- podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1.

Sprostredkovatelia vedú záznamy o všetkých kategóriách spracovateľských činností, ktoré vykonali v mene prevádzkovateľa, pričom tieto záznamy obsahujú:

- meno/názov a kontaktné údaje sprostredkovateľa alebo sprostredkovateľov a každého prevádzkovateľa, v mene ktorého sprostredkovateľ koná, v príslušnom prípade aj zástupcu prevádzkovateľa alebo sprostredkovateľa a meno zodpovednej osoby,
- kategórie spracúvania vykonávaného v mene každého prevádzkovateľa,
- v príslušných prípadoch prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácie vrátane označenia predmetnej tretej krajiny alebo medzinárodnej organizácie a v prípade prenosov uvedených v článku 49 ods. 1 druhom pododseku dokumentáciu primeraných záruk,
- podľa možností všeobecný opis technických a organizačných bezpečnostných opatrení uvedených v článku 32 ods. 1.

V prípade vypracovávania a vedenia záznamov o spracovateľských činnostiach je **z pohľadu malých a stredných podnikov** potrebné uviesť, že tento typ podnikateľských subjektov je **od tejto povinnosti oslobodený, okrem nasledujúcich prípadov**:

- spracovanie osobných údajov môže predstavovať riziko pre práva a slobody dotknutých osôb,
- spracúvanie nie je príležitostné,
- spracovanie zahŕňa osobitné kategórie údajov (OKÚ), ktorými sú: rasový alebo etnický pôvod dotknutej osoby, politické názory dotknutej osoby, náboženské alebo filozofické presvedčenie dotknutej osoby, členstvo v odborových organizáciách, genetické údaje fyzickej osoby, biometrické údaje určené na individuálnu identifikáciu fyzickej osoby, zdravotný stav fyzickej osoby, sexuálny život alebo sexuálna orientácia fyzickej osoby alebo údaje týkajúce sa v súvislosti s dotknutou osobou trestnej činnosti a priestupkov.

1.4.2 Porušenia ochrany osobných údajov

V prípade porušenia ochrany osobných údajov prevádzkovateľ (aj sprostredkovateľ) bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dohliadajúcemu orgánu s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku porušenia práv fyzických osôb. Ak oznámenie nebolo dohliadajúcemu orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania.

V oznámení bude uvedené:

- opis povahy porušenia ochrany osobných údajov,
- podľa možnosti, opis kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- opis pravdepodobných následkov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov,
- podľa potreby, opis opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov.

Ak je pravdepodobné, že porušenie ochrany osobných údajov môže byť vysoko rizikové pre práva fyzickej osoby, musí prevádzkovateľ (aj sprostredkovateľ) okamžite oznámiť túto skutočnosť aj dotknutej osobe.

1.4.3 Posúdenie vplyvu na ochranu údajov

V prípade, ak vplyvom použitia moderných technológií v kontexte povahy, rozsahu, súvislostí a účelu spracovania osobných údajov hrozí vysoké riziko porušenia práv fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Takéto posúdenie sa vyžaduje najmä v prípadoch:

- systematického a rozsiahleho hodnotenia osobných aspektov tykajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania, a z ktorého vychádzajú rozhodnutia s právnymi účinkami tykajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu,
- spracúvania OKÚ vo veľkom rozsahu, vrátane údajov tykajúcich sa uznania viny za trestné činy a priestupky,
- systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Samotné posúdenie obsahuje aspoň:

- systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,
- posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,
- posúdenie rizika pre práva dotknutých osôb,
- opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

Malé a stredné podniky nemajú automatickú povinnosť vykonať posúdenie vplyvu na ochranu údajov. Platí to však len v tom prípade, ak ich činnosť nepredstavuje vysoké riziko pre práva fyzických osôb.

Taký prevádzkovateľ, ktorý na základe posúdenia vplyvu na ochranu údajov zistí, že spracúvanie by mohlo viesť k vysokému riziku v prípade, ak by neprijal opatrenia na zmiernenie tohto rizika, je povinný s dozorným orgánom pred spracúvaním uskutočniť konzultácie. Pre tento účel poskytne prevádzkovateľ dozornému orgánu:

- ak je to nutné, informácie o príslušných povinnostiach prevádzkovateľa, o spoločných prevádzkovateľoch a sprostredkovateľoch zapojených do spracúvania, najmä v prípade spracúvania v rámci skupiny podnikov,
- informácie o účeloch zamýšľaného spracúvania a prostriedkoch na jeho vykonanie,
- informácie o opatreniach a zárukách poskytnutých na ochranu práv dotknutých osôb,
- v príslušných prípadoch kontaktné údaje zodpovednej osoby,
- posúdenie vplyvu na ochranu údajov,
- akékoľvek ďalšie informácie, o ktoré dozorný orgán požiada.

1.4.4 Zodpovedná osoba (DPO)

V súvislosti so spracovávaním osobných údajov by mal prevádzkovateľ aj sprostredkovateľ **určiť zodpovednú osobu**, podliehajúcu priamo najvyššiemu vedeniu subjektu.

Táto povinnosť však nie je z podstaty povinná a netýka sa tak napríklad ani veľkého počtu malých a stredných podnikov.

Priamu povinnosť ustanoviť takúto zodpovednú osobu má subjekt iba vtedy, keď:

- 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,
- hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa, je spracúvanie OKÚ vo veľkom rozsahu, vrátane údajov tykajúcich sa uznania viny za trestné činy a priestupky,
- spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt, s výnimkou súdov pri výkone ich súdnej právomoci.

Zodpovedná osoba má za úlohu poskytovať poradenstvo v oblasti ochrany údajov ostatným zamestnancom subjektu, poskytovať poradenstvo v oblasti posúdenia vplyvov na ochranu údajov, monitorovať opatrenia v súlade s týmto nariadením alebo inými právnym predpismi Únie, resp. štátu, v ktorom je subjekt usadený, plniť úlohy kontaktného miesta pre dozorné orgány a spolupracovať s týmito orgánmi.

1.4.5 Kódexy správania a certifikácia

Členské štáty, dozorné orgány, výbor a Komisia sú podľa nariadenia nabádané **vypracovať kódexy správania** určené na to, aby prispeli k správnemu uplatňovaniu tohto nariadenia, pričom **vezmú do úvahy** osobitné črty rôznych sektorov spracúvania a **osobitné potreby mikropodnikov a malých a stredných podnikov**. **Najmä pre túto kategóriu podnikov je vypracovanie podobných kódexov výhodné, pretože si tak môžu uľahčiť preukazovanie plnenia povinností tohto nariadenia, a to naviac s prihliadnutím na odborové špecifiká.**

Združenia a iné subjekty, zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov, tak môžu vypracovať kódexy správania alebo zmeniť či rozšíriť takéto kódexy napríklad v súvislosti s:

- spravodlivým a transparentným spracúvaním,
- oprávnenými záujmami, ktoré prevádzkovatelia sledujú v konkrétnych situáciách,
- získavaním osobných údajov,
- pseudoanonymizáciou osobných údajov,
- informovaním verejnosti a dotknutých osôb,

- uplatnením práv dotknutých osôb,
- informovaním a ochranou detí a spôsobom získania súhlasu nositeľov rodičovských práv a povinností,
- postupmi zohľadňujúcimi zodpovednosť prevádzkovateľa, opatreniami na špecificky navrhnutú a štandardnú ochranu údajov a opatreniami na zaistenie bezpečnosti spracúvania údajov,
- záväzkom oznamovať porušenia ochrany osobných údajov dozorným orgánom a informovaním dotknutých osôb o takýchto porušeniach ochrany osobných údajov;
- vypracovaním postupu prenosu osobných údajov do tretích krajín alebo nadnárodným organizáciám,
- mimosúdnym konaním a inými postupmi riešenia sporov, zameranými na riešenie sporov medzi prevádzkovateľmi a dotknutými osobami v súvislosti so spracúvaním bez toho, aby boli dotknuté práva týchto osôb,

Okrem kódexov správania podporia členské štáty aj zavedenie certifikačných mechanizmov, pečatí alebo značiek ochrany údajov. Ich získanie má význam z hľadiska preukázania primeraných záruk zabezpečenia osobných údajov mimo iné na prevádzkovateľov, ktorí v rámci svojej organizačnej štruktúry prenášajú údaje do mimoúnijných krajín. Takáto certifikácia je zo strany subjektu dobrovoľná a udeľuje sa na obdobie maximálne troch rokov, s tým, že je ju možné obnoviť vždy na rovnako dlhé obdobie. Pri zavádzaní certifikačných mechanizmov sa zohľadnia špecifické potreby mikropodnikov, ako aj malých a stredných podnikov.

1.4.6 Prenositeľnosť údajov

Nariadenie GDPR upravuje podmienky prenositeľnosti údajov do tretích krajín alebo mimo územia Únie v rámci nadnárodných organizácií tak, že vyžaduje, aby v takejto krajine alebo nadnárodnej organizácií boli splnené podmienky zaručujúce primeranú ochranu údajov.

Za týmto účelom Európska komisia pravidelne monitoruje vývoj v tretích krajinách a nadnárodných organizáciách a na základe získaných informácií, rozhoduje či je daný štátny, medzinárodný alebo komerčný subjekt dôveryhodný.

Prenos údajov v rámci nadnárodného komerčného subjektu je možný okrem splnenia podmienky dôveryhodnosti (ktorá sa musí vzťahovať aj na krajinu, kde je tento subjekt usadený), aj na podmienku poskytnutia primeranej záruky a na podmienku, že dotknuté osoby majú bezpodmienečne k dispozícii vymožiteľné práva a účinné právne prostriedky nápravy. Pod pojmom primerané záruky sa rozumejú najmä:

- záväzné vnútropodnikové pravidlá v súlade s článkom 47 Nariadenia,
- štandardné doložky o ochrane údajov, ktoré prijala Európska komisia alebo dozorný orgán,
- schválené kódexy správania,
- schválené certifikačné mechanizmy,
- zmluvné doložky medzi dotknutými subjektmi z EÚ a príjemcom osobných údajov v tretej krajine.

V prípade, že osobné údaje sa migrujú mimo územia EÚ na základe vnútropodnikových pravidiel, tieto dozorujúci orgán schváli ako vyhovujúci prostriedok len vtedy, ak sú právne

záväzné pre každého člena skupiny podnikov, vrátane ich zamestnancov; a ak sa nimi jasne udeľujú vymáhateľné práva osobám, ktorých osobné údaje sa spracovávajú a migrujú.

1.4.7 Dozorné orgány a sankcie

Ustanovenie jedného alebo viacerých dozorných orgánov verejnej moci, dohliadajúcich na napĺňanie ustanovení nariadenia o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, je v kompetencií každého členského štátu EÚ. Takýto orgán / orgány vykonávajú svoje kompetencie len na území svojho štátu. V Slovenskej republike je dohľadovou činnosťou poverený **Úrad na ochranu osobných údajov**.[15]

Keďže na činnosti verejného dozorného orgánu sa vzťahuje princíp teritoriality, dozorné orgány smú zriaďovať aj hlavné prevádzkarne, a to práve za účelom dohliadania na cezhraničné spracovávanie osobných údajov. Takýto typ dozorného orgánu na úrovni podnikateľského subjektu potom podlieha (ako v oblasti spolupráce, tak aj nahlasovania porušení nariadenia) s verejným dozorným orgánom danej krajiny.

Dozorné orgány majú podľa článku 58 Nariadenia nasledujúce právomoci:

- nariadiť prevádzkovateľovi a sprostredkovateľovi a v príslušnom prípade zástupcovi prevádzkovateľa alebo sprostredkovateľa, aby poskytli všetky informácie, ktoré vyžaduje na plnenie svojich úloh,
- viesť vyšetrovania vo forme auditov v oblasti ochrany údajov,
- vykonávať preskúmania certifikácií vydaných podľa článku 42 ods. 7,
- oznamovať prevádzkovateľovi alebo sprostredkovateľovi údajné porušenie tohto nariadenia,
- získať od prevádzkovateľa a sprostredkovateľa prístup ku všetkým osobným údajom a všetkým informáciám potrebným na plnenie svojich úloh,
- získať prístup do všetkých priestorov prevádzkovateľa a sprostredkovateľa, ako aj k akémukoľvek zariadeniu a prostriedkom na spracúvanie údajov.

Dozorný orgán má podľa článku 58 Nariadenia naviac nasledujúce nápravné právomoci:

- upozorniť prevádzkovateľa alebo sprostredkovateľa na to, že plánované spracovateľské operácie pravdepodobne porušia ustanovenia tohto nariadenia vykonávať preskúmania certifikácií,
- napomenúť prevádzkovateľa alebo sprostredkovateľa, ak spracovateľské operácie porušili ustanovenia tohto nariadenia,
- nariadiť prevádzkovateľovi alebo sprostredkovateľovi, aby vyhovel žiadostiam dotknutej osoby o uplatnenie jej práv podľa tohto nariadenia,
- nariadiť prevádzkovateľovi alebo sprostredkovateľovi, aby svoje prevádzkové operácie zosúladil podľa potreby určeným spôsobom a v rámci určenej lehoty s ustanoveniami tohto nariadenia,
- nariadiť prevádzkovateľovi, aby porušenie ochrany osobných údajov oznámil dotknutej osobe,
- nariadiť dočasné alebo trvalé obmedzenie, vrátane zákazu spracúvania,
- nariadiť opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania podľa článkov 16, 17 a 18 a informovanie príjemcov, ktorým boli osobné údaje poskytnuté o takýchto opatreniach v súlade s článkom 17 ods. 2 a článkom 19,

[15] Webové sídlo: https://dataprotection.gov.sk/sk/

- odňať certifikáciu alebo nariadiť certifikačnému subjektu, aby odňal alebo nevydal certifikáciu vydanú podľa článkov 42 a 43 alebo nariadiť certifikačnému subjektu, aby nevydal certifikáciu, ak nie sú splnené alebo ak už nie sú splnené požiadavky na certifikáciu,
- uložiť v závislosti od okolností každého jednotlivého prípadu správnu pokutu podľa článku 83, a to popri opatreniach uvedených v tomto odseku alebo namiesto nich,
- nariadiť pozastavenie toku údajov príjemcovi v tretej krajine alebo medzinárodnej organizácii.

V prípade, keď sa verejný dozorný orgán domnieva, že je treba naliehavo konať, má právo prijať predbežné opatrenia na dobu maximálne troch mesiacov.

Ak sa verejný dozorný orgán rozhodne udeliť správnu pokutu, musí prihliadať na všetky relevantné súvislosti (úroveň a rozsah, ako aj priťažujúce a poľahčujúce) porušenia tohto nariadenia. **Rovnako musí prihliadať aj na veľkosť a finančné možnosti dotknutého podnikateľského subjektu.**

Na rozdiel od nariadenia NIS2 je v tomto prípade maximálna sankčná čiastka predmetom európskeho práva (tohto nariadenia) a členské štáty tak nemajú právo upraviť si v národnej legislatíve maximálnu výšku správnej finančnej sankcie.

Jednotlivé výšky správnych finančných sankcií sa (aj v Slovenskej republike) odvíjajú od charakteru porušeného ustanovenia.

Za porušenie:

- povinností prevádzkovateľa a sprostredkovateľa,
- povinností certifikačného a monitorujúceho subjektu,

môžu byť uložené správne pokuty až do 10.000.000,- Eur alebo v prípade komerčného subjektu až do 2 % celosvetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá čiastka je vyššia.

Za závažnejšie priestupky, medzi ktoré patria:

- porušenie základných zásad spracúvania vrátanie podmienok súhlasu,
- porušenie práv dotknutých osôb,
- porušenie cezhraničných podmienok prenosu osobných údajov,
- porušenie akýchkoľvek povinností podľa práva členského štátu vo vzťahu k spracúvaniu údajov národného identifikačného čísla, údajov súvisiacich so zamestnaním a údajov na účely archivácie vo verejnom záujme,
- nesplnenie príkazu dozorného orgánu alebo nedodržanie dočasného alebo definitívneho obmedzenia spracúvania alebo pozastavenia tokov údajov nariadeného dozorným orgánom, ako aj neposkytnutie prístupu k údajom,

môžu byť uložené správne pokuty až do 20.000.000,- Eur, alebo v prípade komerčného subjektu až do 4 % celosvetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá čiastka je vyššia.

1.5 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (CSA)

Nariadenie 2019/881 (Akt kybernetickej bezpečnosti) sa venuje dvom tematickým okruhom. Prvý sa týka posilnenia postavenia Agentúry Európskej únie pre kybernetickú bezpečnosť (ďalej ENISA), druhý okruh je venovaný úzko súvisiacej téme certifikácie kybernetickej bezpečnosti IKT.

1.5.1 Agentúra ENISA

Jednotlivé články Nariadenia venované agentúre ENISA jasnejšie a širšie vymedzujú jej úlohy v oblastiach kybernetickej bezpečnosti, a to vo forme:

- odborných konzultácií s organizáciami, inštitúciami EÚ a členskými štátmi,
- poskytovania pomoci s budovaním odborných kapacít na celoeurópskej, aj národných úrovniach,
- manažovania spolupráce na úrovni štátov, ale aj organizácií,
- podpory certifikácie a normalizácie kyberbezpečnosti vo vzťahu k produktom, službám a postupom IKT,
- podpory vzdelávania a informovanosti.

Z obsahu tejto časti nariadenia (ako aj štatútu agentúry, uvedeného v zriaďovacom nariadení (ES) č. 460/2004) je zrejmé, že agentúra ENISA nemá výkonné právomoci a má na európskej úrovni skôr poradnú, analytickú a koordinačnú funkciu. Z pohľadu jej úloh sa tak do činnosti MSP čiastočne premieta oblasť podpory vzdelávania a informovanosti, kde agentúra vypracovala a na svojom webe aj sprístupnila online nástroj[16] na posudzovanie zrelosti kybernetickej bezpečnosti pre MSP. Subjekty tak môžu prostredníctvom neho posúdiť svoju aktuálnu úroveň kybernetickej bezpečnosti, vygenerovať si správu s odporúčaniami a následnými krokmi na zlepšenie bezpečnostných postupov a porovnať úroveň svojej obranyschopnosti s inými spoločnosťami v Európe podľa rozpočtu, veľkosti alebo krajiny.

1.5.2 Certifikácia kybernetickej bezpečnosti

Druhý obsahový okruh nariadenia sa dotýka oblasti pravidiel pre certifikáciu kybernetickej bezpečnosti. Práve jednotné rámce kybernetickej bezpečnosti sú dôležitým nástrojom na ochranu dát, získanie konkurenčnej výhody a splnenie legislatívnych požiadaviek aj pre MSP.

Ciele (tak ako sú uvedené v článku 51 Nariadenia), ktoré sú sledované vytvorením základných rámcov kybernetickej bezpečnosti, sú:

- chrániť uchovávané, prenášané alebo inak spracúvané údaje pred náhodným či neoprávneným uchovávaním, spracúvaním, prístupom alebo poskytnutím počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;
- chrániť uchovávané, prenášané alebo inak spracúvané údaje pred náhodným či neoprávneným zničením, stratou alebo zmenou alebo nedostatočnou dostupnosťou počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;

[16] Uvedený nástroj je po bezplatnej registrácií dostupný na https://tools.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/

- umožňovať oprávneným osobám, programom alebo zariadeniam prístup výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;
- identifikovať a dokumentovať známe závislosti a zraniteľnosti;
- zaznamenávať, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;
- umožňovať overenie, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;
- overovať, či produkty IKT, služby IKT a procesy IKT neobsahujú známe zraniteľnosti;
- v prípade fyzického alebo technického incidentu včas obnoviť dostupnosť údajov, služieb a funkcií a prístup k nim;
- aby produkty IKT, služby IKT a procesy IKT boli bezpečné štandardne a už v štádiu návrhu;
- aby sa produkty IKT, služby IKT a procesy IKT dodávali alebo poskytovali s aktualizovaným softvérom a hardvérom, ktoré neobsahujú verejne známe zraniteľnosti a dodávali alebo poskytovali s mechanizmami na bezpečnú aktualizáciu.

Viaceré z týchto princípov sú detailnejšie rozpracované v Smernici 2022/2555 (NIS2) a Nariadení 2016/679 (GDPR), preto sú bližšie popísané len tie, ktoré neboli spomenuté v dotknutých kapitolách.

Akt kybernetickej bezpečnosti sa mimo iné špecificky zaoberá vytvorením trojúrovňovej certifikácie produktov, služieb a procesov IKT. Je vyjadrená stupňami dôveryhodnosti (základný, pokročilý, vysoký) , ktoré podnikom, vrátane MSP, pomáhajú vybrať si vhodnú úroveň ochrany, a to na základe svojich potrieb a požiadaviek zákazníkov.

Základný stupeň ochrany má poskytovať **bazálnu úroveň ochrany pred bežnými kybernetickými hrozbami**, preto je vhodné ho uplatniť pri základných riešeniach IKT, ktoré nepracujú s citlivými údajmi. Testovanie súladu základného stupňa ochrany s minimálnymi požiadavkami na kybernetickú bezpečnosť sa obvykle realizuje prostredníctvom **samohodnotenia** alebo jednoduchých overovacích postupov. Certifikát so základným stupňom ochrany preto môže MSP poskytovať finančne nenáročný spôsob preukázania súladu s bezpečnostnými normami.

Pokročilý stupeň ochrany chráni pred sofistikovanejšími kybernetickými útokmi a je tak určený pre systémy a služby, ktoré spracovávajú citlivejšie údaje alebo patria do kritickej infraštruktúry. Vyžaduje testovanie a hodnotenie bezpečnostných opatrení nezávislými organizáciami. Z pohľadu MSP má význam získať certifikáciu pokročilého stupňa najmä v prípadoch, kedy poskytujú služby veľkým klientom alebo pracujú s osobnými a obchodne citlivými údajmi.

Vysoký stupeň ochrany pokrýva sofistikované hrozby, často iniciované cudzími a nepriateľskými štátnymi subjektmi. Preto je vhodná pre kritické vládne a armádne aplikácie, v odôvodnených prípadoch aj pre sektory energetiky, či bankovníctva. Certifikačný proces na tento stupeň vyžaduje komplexné testovanie, audity a posúdenia bezpečnostných mechanizmov. Ak MSP nevstupujú do špecificky definovaných obchodných vzťahov s vyššie uvedenými subjektmi, nie je pre ne certifikácia na vysoký stupeň ochrany potrebná.

Konkrétne technické požiadavky jednotlivých stupňov však nie sú priamo uvedené v Nariadení o kybernetickej bezpečnosti, ale sú obsahom konkrétnych certifikačných schém. Tieto má za úlohu vypracovávať práve agentúra ENISA, tak aby určovali technické požiadavky

pre každý stupeň dôveryhodnosti, metodiku testovania a overovania, ako aj požiadavky na audit a hodnotenie.

Aktuálne sú vypracované alebo pripravované schémy certifikácie pre cloudové služby (EUCS), IT produkty (EUCC)[17] a 5G infraštruktúru (EU5G)[18].

K jednotlivým stupňom certifikačných schém stanovených agentúrou ENISA treba poznamenať, že ide o ich minimálnu požadovanú úroveň. V praxi to znamená, že pre jednotlivé stupne certifikácie môže každý členský štát stanoviť vlastné doplnkové požiadavky a/alebo pravidlá. Národný bezpečnostný úrad tak neurobil[19] a certifikačné schémy SR prevzala zatiaľ bezo zmeny.

MSP by mohli využiť aj dostupné schémy a možnosti **čiastočných, resp. modulárnych certifikácií**. Tie umožňujú získať odborné znalosti a kompetencie, postupne, v tzv. moduloch, z ktorých ide vyskladať certifikáciu na individuálnu požadovanú úroveň. Výhodou tohto postupu je nielen okamžitá nižšia finančná náročnosť a kratší čas potrebný na dokončenie jednotlivých modulov, ale aj flexibilita, keďže je možné takto získať konkrétne zručnosti bez potreby absolvovať ucelený rozsiahly kurz.

V praxi možno použiť napríklad tieto modulárne certifikácie:

- **ISC2 Certified in Cybersecurity (CC)** - základný certifikát, ku ktorému je neskôr možné nadstavovať ďalšie certifikácie, vrátane špičkových, ako napr. CISSP.
- **Cisco CyberOps Associate/Professional** - umožňuje postupne získavať zručnosti v oblasti sieťovej bezpečnosti.
- **GIAC Modular Certifications** - ponúka certifikácie pre viaceré konkrétne oblasti ako napr. manažment bezpečnosti, bezpečnosť cloudových prostredí, sieťová bezpečnosť a iné.
- **Microsoft Security, Compliance, and Identity Certifications** - ponúka základné aj pokročilé moduly zamerané na technológie spoločnosti Microsoft.

[17] https://www.enisa.europa.eu/sites/default/files/publications/ENISA_candidate%20scheme_EUCC.pdf
[18] K februáru 2025 vo finálnej fáze prípravy - https://www.enisa.europa.eu
[19] Stav k februáru 2025

1.6 Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 o jednotnom trhu s digitálnymi službami (DSA)

Akt o digitálnych službách je uceleným právnym rámcom zameraným na oblasť regulácie digitálnych služieb, poskytovaných informačnými spoločnosťami (resp. online platformami). Tieto sú definované ako subjekty poskytujúce za úhradu elektronické služby na diaľku, prostredníctvom individuálnej žiadosti príjemcu (zákazníka). V praxi ide o široký diapazón služieb, ako sú sociálne siete, rezervačné systémy, internetové obchody, streamovacie služby, online spravodajské portály, online bankovníctvo a iné. Poskytnutou digitálnou službou sa na účely tohto nariadenia rozumejú obyčajný prenos služby, dočasné uchovávanie údajov zákazníka a hosting webových stránok a súborov na serveroch.

Okruhy problematík, ktorým sa z pohľadu MSP Akt o digitálnych službách venuje, sú regulácie povinností poskytovateľov sprostredkovateľských služieb a opatrenia na ochranu spotrebiteľov, transparentnosť online reklamy a v neposlednom rade aj oblasť dohľadu a sankcií.

1.6.1 Povinnosti poskytovateľov sprostredkovateľských služieb

Povinnosti poskytovateľov sprostredkovateľských služieb a opatrenia na ochranu spotrebiteľov sa viažu predovšetkým k zavedeniu mechanizmov na odstraňovanie nezákonného obsahu a na zabezpečenie transparentnosti procesov moderovania obsahu. Tieto povinnosti sú viazané na všetkých sprostredkovateľov (**vrátane tých spomedzi MSP**).

Poskytovatelia sprostredkovateľských služieb sú podľa nariadenia povinní vytvoriť jednotné kontaktné miesto pre zákazníkov, oznamovateľov porušení, ako aj pre dohliadajúce orgány. V súvislosti s poskytovanou službou verejne a zrozumiteľne uvedú obmedzenia, ktoré sa vzťahujú na informácie poskytované zákazníkmi. Tieto informácie musia zahŕňať popisy všetkých politík, postupov, opatrení a nástrojov používaných na účely moderovania obsahu, vrátane algoritmického rozhodovania a ľudskej kontroly, ako aj o rokovacom poriadku ich vnútorného systému vybavovania sťažností. Na všetky spomínané ustanovenia sa zvlášť dbá, ak je služba zameraná alebo ju v prevažnej miere využívajú maloletí. Všetky informácie musia byť v tomto prípade zverejnené tak, aby im maloletí rozumeli.

Všetci poskytovatelia sprostredovateľských služieb spomedzi **stredných podnikov**[20] sú aspoň raz ročne **povinní verejne poskytovať** aj správy o transparentnosti. Ich obsahom je za sledované obdobie zverejnenie:

- počtu príkazov vydaných od dohliadajúcich orgánov pre poskytovateľov sprostredkovateľských služieb rozdelených podľa druhu nezákonného obsahu, štátu EÚ z ktorého príkaz pochádza a mediáne času potrebného na informovanie dohliadajúceho orgánu o prijatí príkazu a jeho vykonaní,
- počtu podnetov prijatých od oznamovateľov, rozdelených podľa druhu údajného nezákonného obsahu, prijatých opatreniach rozdelených podľa toho či boli prijaté na základe zákona alebo obchodných podmienok, počtu podnetov vyriešených automatizovanými prostriedkami (AI) a o mediáne času potrebnom na prijatie opatrení,
- informácií od poskytovateľov sprostredkovateľských služieb o moderovaní obsahu z vlastnej iniciatívy (vrátane používania automatizovaných nástrojov), opatrení prijatých na poskytovanie odbornej prípravy a pomoci osobám zodpovedným za moderovanie obsahu, počtu

[20] Nevzťahuje sa na malé podniky a mikropodniky.

a druhu prijatých opatrení, ktoré ovplyvňujú dostupnosť, viditeľnosť a prístupnosť informácií poskytovaných príjemcami služby a schopnosti príjemcov poskytovať informácie prostredníctvom služby, ako aj o iných súvisiacich obmedzeniach služby, rozdelených podľa druhu nezákonného obsahu alebo porušenia obchodných podmienok, podľa metódy detekcie a druhu prijatého obmedzenia,

- informácií od poskytovateľov sprostredkovateľských služieb a hostingových služieb o počte sťažností prijatých prostredníctvom vnútorných systémov vybavovania sťažností v súlade s obchodnými podmienkami, prijatých rozhodnutiach, mediáne času potrebnom na prijatie rozhodnutí a počte prípadov, v ktorých boli rozhodnutia zrušené,
- informácií o akomkoľvek použití automatizovaných prostriedkov na účely moderovania obsahu vrátane kvalitatívneho opisu, špecifikácii presných účelov, ukazovateľov presnosti a možnej chybovosti automatizovaných prostriedkov a akýchkoľvek naň uplatnených záruk,
- počte sporov predložených orgánom mimosúdneho riešenia sporov, výsledky riešenia sporov a medián času potrebný na dokončenie postupov riešenia sporov, ako aj podiel sporov, v prípade ktorých poskytovateľ online platformy vykonal rozhodnutia orgánu,
- počte pozastavení poskytovania služby, rozdelených na pozastavenia uložené za poskytovanie zjavne nezákonného obsahu, predkladanie zjavne neopodstatnených oznámení alebo zjavne neopodstatnených sťažností.

Mimo to, raz za šesť mesiacov poskytovatelia sprostredovateľských služieb uverejnia pre každú online platformu na verejne prístupnej časti svojho rozhrania informáciu o priemernom mesačnom počte aktívnych používateľov svojej služby v EÚ za posledných šesť mesiacov.[21] Dôvodom takého postupu je priebežné overovanie, či sprostredkovateľ dosiahol priemerný mesačný počet používateľov 45.000.000. Po dosiahnutí tejto hranice sa podľa nariadenia budú na takéhoto sprostredkovateľa vzťahovať výrazne prísnejšie podmienky.

Poskytovatelia hostingových služieb (**aj spomedzi malých a stredných podnikov**) sú povinní zaviesť verejne a výlučne elektronicky dostupné mechanizmy, ktoré jednotlivcom aj subjektom umožnia oznamovať informácie obsahujúce potenciálne nezákonný obsah.

Formuláre určené pre takéto podania by mali obsahovať nasledujúce prvky:

- dôvody, prečo si oznamujúca osoba alebo subjekt myslí, že ide o nezákonný obsah,
- presná adresa URL a podľa potreby aj bližšie označenie informácií umožňujúcich identifikovanie nezákonného obsahu,
- meno a e-mailovú adresu oznamujúcej osoby alebo subjektu, kam poskytovateľ odošle správu o prijatí oznámenia, rozhodnutí a prijatých opatreniach,
- vyhlásenie dobrej vôle jednotlivca alebo subjektu, že informácie a tvrdenia ktoré v podaní poskytol sú pravdivé, úplné a presné.

V prípadoch, ak poskytovatelia hostingových služieb obmedzia viditeľnosť príjemcom zverejnených informácií (vrátane ich odstránenia alebo znemožnenia prístupu k nim), obmedzia v akomkoľvek rozsahu užívateľovi služby, peňažné platby, úplne alebo čiastočne pozastavia alebo ukončia poskytovanie služby alebo mu zblokujú či zrušia účet, sú povinní poskytnúť užívateľovi služby zdôvodnenie. To by malo obsahovať najmenej:

[21] Podľa čl. 33 ods. 3 Nariadenia o digitálnych službách (DSA). K 1.3 2025 predmetný odsek neposkytuje nijaký presný vzorec na výpočet a aktívneho príjemcu služby definuje ako používateľa, ktorý sa pripojil k službe aspoň raz za daný mesiac. Európska komisia môže do budúcnosti vydať usmernenia alebo metodiky pre výpočet tohto čísla.

- správu o charaktere a rozsahu reštrikcie vo vzťahu k viditeľnosti informácie alebo peňažných tokov, prípadne či sú uložené aj iné reštrikčné opatrenia a ak je to potrebné, aj ich územnú a časovú platnosť,
- skutočnosti a okolnosti, ktoré viedli k prijatiu rozhodnutia, vrátane informácie či bolo prijaté na základe externého podania, vnútorného vyšetrovania alebo podnetu od automatizovaného prostriedku,
- v prípade, ak ide o nezákonný obsah, prečo je za takýto považovaný a na akom právnom základe,
- v prípade, ak boli zverejnením informácií porušené obchodné podmienky poskytovateľa hostingových služieb, odkaz na porušený článok tohto dokumentu a dôvod prečo informácie tento článok porušujú,
- informácie o prostriedkoch nápravy, ktoré ma užívateľ k dispozícii, a to ako v rámci interných mechanizmov vybavovania sťažností a iných mimosúdnych riešení, tak aj riešenia prostredníctvo súdu.

Nariadenie ďalej spresňuje postup na uplatnenie prostriedkov nápravy. Predovšetkým vymedzuje časové obdobie najmenej šiestich mesiacov po obmedzení služby, počas ktorých má užívateľ služby možnosť vzniesť námietku. Rovnako poskytovateľovi určuje povinnosť poskytnúť súčinnosť akémukoľvek oprávnenému orgánu mimosúdneho riešenia sporov, ktorého si zvolil užívateľ.[22]

V prípadoch, ak poskytovatelia hostingových služieb majú podozrenie na spáchanie trestného činu, tieto informácie sú povinní okamžite oznámiť orgánom činným v trestnom konaní.

Poskytovatelia online platforiem, ktorí umožňujú uzatvárať spotrebiteľom zmluvy na diaľku, musia podľa nariadenia zaviesť opatrenia vo vzťahu k overeniu obchodníkov, ktorým poskytujú svoje sprostredkovateľské služby.[23]

Nariadenie určuje poskytovateľom online platforiem povinnosti týkajúce sa aj **transparentnosti online reklamy**. Poskytovatelia online platforiem musia zabezpečiť, aby užívatelia služieb mohli jasne identifikovať:

- že prezentované informácie sú reklamou,
- fyzickú alebo právnickú osobu, v mene ktorej sa reklama prezentuje,
- fyzickú alebo právnickú osobu, ktorá reklamu zaplatila, ak je odlišná od predchádzajúcej,
- hlavné parametre použité na určenie príjemcu, ktorému sa reklama zobrazuje a informácie o možnostiach zmeny týchto parametrov.

Ak poskytovateľ používa na svojej platforme odporúčací systém (tzv. kontextovú reklamu), je povinný užívateľom zdôvodniť podľa akých kritérií tento odporúčací systém funguje a dôvody prečo sú tieto kritéria považované za rozhodujúce. Zároveň musí užívateľovi poskytnúť možnosť na úpravu alebo ovplyvňovanie týchto parametrov.

[22] Nevzťahuje sa na malé podniky a mikropodniky.
[23] Nevzťahuje sa na malé podniky a mikropodniky.

1.6.2 Dohľad a sankcie

Členský štát musí určiť orgán dohľadu nad poskytovateľmi sprostredkovateľských služieb. V SR vykonáva túto funkciu **Rada pre mediálne služby** [24].

Určenie výšky sankcií za konkrétne nedodržanie povinností uvedených v Akte o digitálnych službách je v kompetencií jednotlivých členských štátov EÚ. Ich maximálna výška v SR zodpovedá najvyššej možnej sume z tohto Nariadenia a ide teda o **6 % ročného svetového obratu dotknutého poskytovateľa sprostredkovateľských služieb za predchádzajúce účtovné obdobie**. Za poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií, neposkytnutie odpovede alebo neopravenie nesprávnych, neúplných alebo zavádzajúcich informácií, ako aj za nepodrobenie sa kontrole, je maximálna suma pokuty **do 1 % ročného príjmu alebo svetového obratu za predchádzajúce účtovné obdobie**. V prípade uplatnenia penále, toto môže dosahovať maximálne 5 % priemerného denného svetového obratu alebo príjmu za predchádzajúce účtovné obdobie. Penále sa vypočítava od dátumu vydania príslušného rozhodnutia.

[24] Webové sídlo dostupné na: https://rpms.sk

1.7 Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA)

Cieľom Nariadenia 2002/2554 o digitálnej prevádzkovej odolnosti finančného sektora (ďalej DORA) je zabezpečiť, aby finančné inštitúcie v EÚ boli schopné **odolávať a reagovať na incidenty IKT a zotaviť sa z nich. Upravuje takisto požiadavky na riadenie rizík** IKT, nahlasovanie incidentov, testovanie bezpečnosti a dohľad nad poskytovateľmi IKT služieb.

Do pôsobnosti nariadenia spadajú okrem bánk, poisťovní a investičných spoločností aj poskytovatelia kryptoaktív, správcovia alternatívnych investičných fondov, sprostredkovatelia úverov, ale napríklad aj externí poskytovatelia IKT služieb.

Naopak, **nariadenie DORA sa nevzťahuje na sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia**, **ktorí spĺňajú parametre malých a stredných podnikov**.

1.7.1 Riadenie rizík

Ohľadom **riadenia rizík v oblasti IKT** stanovuje nariadenie DORA povinnosti finančných subjektov dohliadať na svoju digitálnu prevádzkovú odolnosť a určuje aj spôsoby, ako majú identifikovať, riadiť a zmierňovať riziká spojené s IKT.

Na riadenie rizík musia zaviesť komplexný a odolný rámec, ktorý zahŕňa procesy identifikácie, ochrany, detekcie, reakcie a obnovy pri kybernetických útokoch alebo výpadkoch systémov, a to tak, aby bola zabezpečená nepretržitá dostupnosť infraštruktúry IKT.

Za oblasť riadenia rizík je priamo zodpovedné vedenie finančného subjektu a zodpovedá tak aj za osoby poverené monitorovaním rizík. Všetky osoby dohliadajúce na systémy IKT (vrátane vedenia) sa musia pravidelne vzdelávať v oblastiach najaktuálnejších trendov kybernetickej bezpečnosti. Zároveň musia zabezpečiť aspoň raz ročne, zdokumentovanie a prípadnú aktualizáciu rámca riadenia IKT rizika.

Finančné subjekty sú povinné identifikovať všetky úlohy, funkcie a povinnosti podporované IKT a následne identifikujú všetky zdroje rizík, a to predovšetkým vo vzťahu k iným finančným inštitúciám a externým dodávateľom služieb. V prípade významnejšej zmeny infraštruktúry siete a informačných systémov je potom nutné vykonať nové posúdenie rizík.

V oblasti **ochrany a prevencie** musia finančné subjekty definovať opatrenia na ochranu IKT, s cieľom minimalizovať riziká a zabezpečiť ich bezpečnosť, kontinuitu a odolnosť. Mali by k ním patriť neustále **monitorovanie a kontrola** funkčnosti systémov IKT, navrhovanie a implementácie stratégií a politík na ochranu kritických IKT systémov a údajov, **používanie vhodných IKT technológií a** navrhnutie sietí tak, aby umožňovali rýchle odpojenie alebo segmentáciu pri detegovaní bezpečnostných hrozieb.

Finančné subjekty musia byť schopné rýchlej **detekcie** anomálnych správaní systémov IKT, najmä vo vzťahu ku kybernetickým útokom. V súvislosti s tým musia vedieť identifikovať potenciálne miesta zlyhania systémov IKT.

Schopnosť **reakcie a obnovy** predpokladá, že finančné subjekty musia mať stanovené stratégie na udržanie a obnovu IKT systémov pri incidente, postupy na riešenie výpadkov a

kybernetických útokov, plány na pravidelné ročné testovania a revízie plánov kontinuity a obnovy systému, hodnotenia dopadov narušenia IKT systémov na podnikanie, postupy informovania interných aj externých dotknutých subjektov a schopnosť reportovať náklady a straty spôsobené závažnými IKT incidentmi.

Pre obnovu systémov je takisto dôležité vypracovať politiky zálohovania údajov (vrátane frekvencie a ich rozsahu) a oddelenie záložných systémov od primárnych, tak aby sa zaistila bezpečnosť a integrita údajov. Pri incidente je takisto nutné určiť časové ciele obnovy a dodatočnú kontrolu integrity údajov.

1.7.2 Incidenty súvisiace s IKT

Pre minimalizáciu dopadov incidentov a ich prevenciu je potrebné vypracovať postupy aj pre detekciu, riešenie a oznamovanie incidentov. Finančné subjekty sú povinné zaznamenávať **všetky incidenty a kybernetické hrozby,** s cieľom podrobiť analýze hlavné príčiny a následne implementovať **opatrenia na zabránenie recidívam.**

V procese riadenia incidentov musia finančné inštitúcie uplatňovať štruktúrovaný postup:

- včasné varovanie na základe mechanizmov rýchlej identifikácie hrozieb,
- kategorizáciu incidentov podľa priority, závažnosti a vplyvu,
- pridelenie úloh a povinností dohliadajúcim osobám a zodpovedajúcim organizačným útvarom,
- určenie spôsobu informovania zamestnancov, zákazníkov a médií,
- nahlasovanie závažných incidentov a prijatých opatrení vedeniu,
- plán opatrení na zmiernenie následkov, vrátane obnovy služieb.

Nariadenie DORA stanovuje kritériá na základe ktorých finančné inštitúcie **klasifikujú** závažnosť **incidentov** súvisiacich s IKT. Týmito kritériami sú:

- počet a význam postihnutých klientov/protistrán a objem transakcií,
- trvanie incidentu a výpadku služieb,
- geografický dosah, najmä v prípadoch ak sa dotkne viac ako 2 členských štátov,
- strata údajov a narušenie ich dostupnosti, integrity alebo dôvernosti,
- rozsah postihnutých služieb a transakcií,
- hospodársky dopad a priame i nepriame náklady a straty v dôsledku incidentu.

Klasifikácia závažnosti **kybernetických hrozieb** je realizovaná na základe významu služieb, ktoré sú ohrozené.

V nadväznosti na Nariadenie DORA vypracovali Európska centrálna banka a agentúra ENISA regulačné technické predpisy, ktorými sa presnejšie klasifikujú incidenty a hrozby súvisiace s IKT[25].

Finančná inštitúcia je povinná **nahlasovať závažné incidenty súvisiace s IKT** jedinému určenému hlavnému dohliadajúcemu orgánu v tej členskej krajine EÚ, kde pôsobí. V prípade

[25] **Nariadenie Komisie (EÚ) 2024/1772 z 15. marca 2024,** ktorým sa stanovujú regulačné technické predpisy o klasifikačných kritériách a prahových hodnotách závažnosti pre hlásenie závažných incidentov súvisiacich s IKT podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202401772

Slovenskej republiky je to **Národný bezpečnostný úrad**. Nahlasovanie incidentov môže byť outsorcované na externých poskytovateľov služieb, ale **za ich vecnú aj formálnu správnosť, ako aj včasné podanie, je plne zodpovedná samotná finančná inštitúcia.**

Hlásenia musia byť podávané podľa určených vzorov[26]**,** pričom v prípade technických problémov je možné ich podať v alternatívnej forme. Vždy však musia obsahovať údaje potrebné na **posúdenie významnosti incidentu a jeho cezhraničných vplyvov.**

V prípadoch ak incident ovplyvňuje **finančné záujmy klientov,** finančný subjekt ich musí **bezodkladne** informovať. V prípadoch **významných kybernetických hrozieb** musia byť klienti informovaní o možných **ochranných opatreniach.**

Finančné inštitúcie sú v súvislosti s incidentmi povinné predkladať národnému dohliadajúcemu orgánu tieto typy správ:

- počiatočné oznámenie,
- **priebežné správy,** podávané pri výrazných zmenách stavu incidentu,
- **záverečnú správu,** podávanú po analýze hlavných príčin a dopadov incidentu.

1.7.3 Testovanie digitálnej prevádzkovej odolnosti

Finančné subjekty musia vytvoriť, udržiavať a pravidelne aktualizovať program testovania digitálnej prevádzkovej odolnosti, ktorý zahŕňa rôzne posúdenia, testy, metodiky, postupy a nástroje, aplikovateľné podľa stanovených pravidiel. Testovanie musí byť vykonávané s ohľadom na riziká, špecifické ohrozenia a kritickosť informačných systémov a poskytovaných služieb. Tie IKT systémy a aplikácie, ktoré podporujú kritické alebo dôležité funkcie systému, musia byť testované aspoň raz ročne. Pre prípad, ak sa počas testovania objavia problémy, finančná inštitúcia musí mať vypracovaný postup na určenie priorít, klasifikáciu a nápravu problémov.

V rámci programu testovania sa musia vykonávať rôzne testy a analýzy, vrátane vyhľadávania zraniteľnosti, analýzy otvorených zdrojov, posúdenia bezpečnosti sietí, analýzy nedostatkov, preskúmania fyzickej bezpečnosti, skenovania softvérových riešení, preskúmania zdrojového kódu, testovania výkonnosti a kompatibility, ako aj testovania koncových bodov.

Finančné subjekty sú podľa nariadenia DORA povinné vykonávať každé tri roky pokročilé penetračné testovanie založené na konkrétnych hrozbách (TLPT)[27]. Do testovania musia byť zapojení aj externí poskytovatelia IKT služieb, ak poskytujú služby podporujúce kritické funkcie prevádzkovaných systémov. O tom, ktoré subjekty podliehajú povinnosti realizovať TLPT testovania, rozhoduje príslušný orgán danej krajiny EÚ, ktorým je v SR Národná banka Slovenska.

V súvislosti s MSP je však nutné poznamenať, že v odôvodnení Nariadenia DORA sa zdôrazňuje potreba zohľadniť rozdiely medzi finančnými subjektmi, pokiaľ ide o ich veľkosť a celkový rizikový profil. To znamená, že pri implementácii rámca riadenia rizík IKT by MSP mali zohľadniť rovnováhu medzi svojimi potrebami v oblasti IKT a svojou veľkosťou, ako aj

[26] Nahlasovanie závažných kybernetických bezpečnostných incidentov podľa určeného vzoru je možné na tejto webovej adrese: https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html
[27] Články 26 a 27 Nariadenia DORA upresňujú všetky povinnosti v súvislosti s testovaním TLPT.

povahou a zložitosťou svojich služieb. **Pre väčšinu MSP teda nemusí byť testovanie TLPT povinné.**

1.7.4 Riadenie externého rizika IKT

Nariadenie DORA ukladá **všetkým finančným subjektom** vypracovanie postupov pre bezpečné a kontrolované využívanie externých IKT služieb. Finančné subjekty sú tak povinné do stratégie riadenia rizík IKT:

- zahrnúť viacdodávateľský prístup pri kritických alebo dôležitých funkciách, tak aby finančný subjekt nebol podľa možnosti nadmerne závislý od jedného dodávateľa externých služieb IKT,
- viesť a aktualizovať register všetkých zmlúv s externými poskytovateľmi služieb IKT,
- podávať pravidelné hlásenia orgánom dohľadu,
- **pred uzavretím zmluvy s externým poskytovateľom** posúdiť kritickosti a riziká zmluvného vzťahu, vrátane prípadných subdodávateľských reťazcov obzvlášť, ak pochádzajú z krajín mimo EÚ),
- realizovať pravidelné audity podľa audítorských štandardov,
- zmluvné stanovenie jasných práv a povinností externého poskytovateľa služieb IKT písomnou formou,
- vypracovať stratégie ukončenia zmluvného vzťahu, vrátane alternatívnych riešení.

1.7.5 Dohľad a sankcie

Vo vzťahu ku kritickým externým poskytovateľom služieb IKT Nariadenie upravuje aj pravidlá a rámec dohľadu nad ich činnosťou. Vymedzuje postup určovania kritických externých poskytovateľov, kritériá hodnotenia ich dôležitosti pre finančné subjekty, úlohy a právomoci hlavných orgánov dohľadu a štruktúru dozoru. Definuje tiež povinnosti týchto poskytovateľov, mechanizmy oznámenia ich statusu a požiadavky na spoluprácu medzi európskymi orgánmi dohľadu.

V prípade úplného alebo čiastočného nedodržiavania opatrení externým poskytovateľom služieb IKT na informovanie a/alebo umožnenie kontroly zo strany hlavného orgánu dozoru, Nariadenie DORA umožňuje udeliť takémuto subjektu platbu pravidelného penále až do dosiahnutia kooperačného súladu. Penále je stanovené **za každý deň vo výške najviac 1 % jeho priemerného denného celosvetového obratu v predchádzajúcom finančnom roku.**

1.8 Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (CRA)

Nariadenie 2024/2847, známe ako Akt o kybernetickej odolnosti (ďalej CRA), je dokument zameraný na stanovenie pravidiel pre kybernetickú bezpečnosť hardvérových a softvérových produktov s digitálnymi prvkami (ďalej produkty), ktoré sú uvádzané alebo prístupné na trhu EÚ. Primárne sa teda týka výrobcov takýchto produktov, ale rozsah dotknutých subjektov sa rozširuje aj o dovozcov, distribútorov a poskytovateľov softvérových a hardvérových produktov.

Výrobcovia musia u svojich produktov zabezpečiť súlad so základnými požiadavkami na kybernetickú bezpečnosť[28]. V súlade s týmito požiadavkami musia byť aj ďalšie požadované postupy výrobcu[29]. Nariadenie CRA takisto definuje dôležité a kritické produkty s digitálnymi prvkami, ktoré podliehajú prísnejším posudzovaniam zhody.

Dôležité produkty musia vykonávať funkcie[30], ktoré sú kritické pre kybernetickú bezpečnosť (napr. autentifikácia, ochrana siete, bezpečnosť koncových bodov, atď.), alebo **môžu** vykonávať funkcie, ktoré predstavujú veľké riziko pre iné produkty alebo používateľov (napr. centrálne riadenia siete, spracovania osobných údajov, atď.).

Kritické produkty sú také, od ktorých sú v menšej či väčšej miere závislé kľúčové subjekty (napr. podniky kritickej infraštruktúry) alebo zraniteľnosti nimi poskytovaných produktov by mohli viesť k vážnemu narušeniu **kritických dodávateľských reťazcov** v rámci celého trhu EÚ. Kritické produkty[31] preto podliehajú potrebe získania **európskeho certifikátu kybernetickej bezpečnosti**, a to minimálne na úrovni „VÝZNAMNÁ ZÁRUKA“.[32]

V súvislosti s rozvojom umelej inteligencie sú novo definované aj požiadavky na kybernetickú bezpečnosť produktov kategórie vysokorizikových systémov AI[33]. Systémy AI, sú považované za vyhovujúce, ak spĺňajú požiadavky a postupy na zaistenie základnej bezpečnosti [27, 28] a sú odolné voči chybám, poruchám a neoprávneným zásahom[34].

1.8.1 Povinnosti výrobcov, dovozcov a distribútorov

Výrobcovia sú podľa nariadenia CRA povinní zaručiť, že výrobky s digitálnymi prvkami sú navrhnuté a uvedené na trh v súlade s požiadavkami na kybernetickú bezpečnosť, čím sa minimalizujú riziká a zvyšuje bezpečnosť používateľov. Hlavným povinnosťami výrobcov tak sú:

- Výrobcovia musia pred uvedením produktu na trh vykonať posúdenie rizík spojených s digitálnymi prvkami. Týka sa to aj celého obdobia podpory produktu.

[28] Základné požiadavky sú stanovené v prílohe I, časť I, Nariadenia 2024/2847.
[29] Požiadavky na riešenie zraniteľností sú stanovené v prílohe I, časť II Nariadenia 2024/2847.
[30] Funkcie definujúce dôležité produkty sú uvedené v prílohe III Nariadenia 2024/2847. Do 11. 12. 2025 bude prijatý vykonávací akt, ktorý presnejšie vymedzí ich technické detaily.
[31] Kritické produkty sú definované v prílohe IV III Nariadenia 2024/2847. Ich zoznam podlieha zmenám a doplneniam.
[32] Európska komisia prijme v budúcnosti delegované akty, ktorými určí produkty, podliehajúce získaniu certifikátu na úrovni Významná záruka.
[33] Podľa nariadenia (EÚ) 2024/1689
[34] Podľa článku 15, Nariadenia 2024/1689

- Ak výrobca integruje do produktu komponenty tretích strán (vrátane slobodného softvéru a softvéru s otvoreným zdrojovým kódom), musí zabezpečiť, že nedôjde k ohrozeniu kybernetickej bezpečnosti používateľa. Ak výrobca identifikuje zraniteľnosť komponentu, informuje o tom jeho producenta.
- Výrobca musí určiť obdobie podpory produktov najmenej na päť rokov a zabezpečiť, aby bezpečnostné aktualizácie boli k dispozícii minimálne desať rokov.
- Výrobca musí byť pripravený poskytnúť potrebné informácie orgánom dohľadu nad trhom.
- Výrobca na produkte a v sprievodnej dokumentácií musí uviesť svoje meno, kontaktné údaje a kópiu vyhlásenia EÚ o zhode.
- Výrobca musí poskytnúť zrozumiteľné informácie a návody pre používateľov týkajúce sa inštalácie, používania a podpory produktov.
- Výrobca musí zriadiť kontaktné miesto, kde používatelia budú nahlasovať zraniteľnosti a problémy s produktmi.
- Výrobca musí každú aktívne zneužitú zraniteľnosť alebo incident, oznámiť prostredníctvom jednotnej oznamovacej platformy[35]národnému koordinátorovi CSIRT a agentúre ENISA. V rámci procesu oznamovania je výrobca povinný vydať prvé varovanie do 24 hodín, do 72 hodín detailnejšie informácie (ak sú dostupné) a do 14 dní záverečnú správu s opisom zraniteľnosti, útočníkov (ak sú známi) a nápravných opatrení.
- Výrobca musí informovať o bezpečnostných hrozbách a opatreniach na ich zmiernenie aj postihnutých užívateľov.

Dovozcovia sú podľa nariadenia CRA povinní uvádzať na trh iba produkty, ktoré spĺňajú základné požiadavky kybernetickej bezpečnosti[36] a ich výrobca zaviedol náležité postupy.[37] **Pred uvedením produktu na trh si musia dovozcovia overiť,** že výrobca vykonal posúdenie zhody a má označenie vyhlásenia o zhode CE a EÚ, vypracoval technickú dokumentáciu, prípadne splnil ďalšie špecifické požadované povinnosti uvedené v predchádzajúcom odseku.

Dovozcovia sú takisto povinní uchovávať kópiu vyhlásenia EÚ o zhode najmenej desať rokov a ak výrobca ukončí činnosť, o tejto skutočnosti musia informovať orgány dohľadu.

Rovnako ako výrobcovia, aj dovozcovia sú povinní uviesť na produkte svoje meno a adresu.

Distribútori majú podľa nariadenia CRA obdobné povinnosti ako dovozcovia.

Ak dovozca alebo distribútor (resp. iná fyzická alebo právnická osoba) uvedie na trh produkt pod svojim menom alebo produkt významne upraví, bude považovaná za jeho výrobcu.

1.8.2 Správa softvérov s otvoreným zdrojovým kódom

Organizácie, alebo jednotlivci, ktorí sú zodpovední za správu (vývoj a údržbu) softvérov s otvoreným zdrojovým kódom musia overiteľným spôsobom vytvoriť a zdokumentovať svoju bezpečnostnú politiku. Táto musí podporovať bezpečný vývoj produktov s digitálnymi prvkami, riešenie a dobrovoľné oznamovanie zraniteľností a podporovať výmenu informácií v open-source komunite.

[35] Nahlasovanie závažných kybernetických bezpečnostných incidentov podľa určeného vzoru je možné na tejto webovej adrese: https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html
[36] Príloha I, časť I, Nariadenia 2024/2847.
[37] Príloha I, časť II Nariadenia 2024/2847.

Ak sa správcovia softvérov s otvoreným zdrojovým kódom podieľajú na ich vývoji, musia každú aktívne zneužitú zraniteľnosť oznámiť dohliadajúcemu orgánu podobne ako výrobca, a to aj s dodržaním časovej postupnosti prvého varovania (do 24h.), detailov (do 72h.) a záverečnej správy (do 14 dní). V prípade, ak ide o závažné incidenty, sú takisto povinní informovať aj agentúru ENISA a užívateľov svojich produktov (vrátane opatrení na ich zmiernenie).

Rovnako majú po výzve dohliadajúceho orgánu povinnosť poskytnúť mu súčinnosť pri zmierňovaní kyberneticko-bezpečnostných rizík a poskytnúť mu príslušnú dokumentáciu v zrozumiteľnom jazyku, a to v papierovej alebo elektronickej forme.

1.8.3 Označenie o zhode a technická dokumentácia

Ak produkt s digitálnymi prvkami spĺňa európske normy, musí na ňom byť umiestnené viditeľné a nezmazateľné označenie CE, s veľkosťou najmenej 5 mm. Ak typ produktu neumožňuje toto označenie umiestniť priamo naň, môže byť umiestnené na obale alebo vo vyhlásení o zhode. Pri softvérových produktoch sa môže uviesť vo vyhlásení o zhode alebo na webovej stránke softvérového produktu. Ak produkt prešiel posudzovaním zhody, musí byť pri označení CE aj identifikačné číslo organizácia vykonávajúcej toto posudzovanie (notifikovaná osoba). **Notifikovanou osobou** je nezávislá organizácia alebo inštitúcia, ktorú členský štát Európskej únie poveril vykonávaním posudzovania zhody produktov s požiadavkami stanovenými v právnych predpisoch EÚ.

Technická dokumentácia k produktu musí obsahovať[38] všetky potrebné údaje a detaily o opatreniach, ktoré výrobca zaviedol na zabezpečenie zhody produktu s požiadavkami kybernetickej bezpečnosti. Jej súčasťou musí byť aj vyhlásenie o zhode produktu s požiadavkami kybernetickej bezpečnosti[39].

Výrobca musí overiť, či produkt a jeho výrobný proces spĺňajú základné požiadavky kybernetickej bezpečnosti podľa jedného z nasledujúcich postupov:

- **Modul A**: postup vnútornou kontrolou[40],
- **Modul B + Modul C**: postup EÚ skúškou typu a vnútornou kontrolou výroby[41],
- **Modul H**: Posudzovanie zhody založené na úplnom zabezpečení kvality[42],
- Ak je uplatniteľná, **Európskou schémou certifikácie kybernetickej bezpečnosť.**

Nariadenie CRA odporúča členským štátom aj **špecifickú podporu MSP v podobe školení,** ktoré na Slovensku pripravujú Kompetenčné a certifikačné centrum kybernetickej bezpečnosti alebo Národný bezpečnostný úrad. MSP budú môcť naviac **predkladať technickú dokumentáciu v zjednodušenom formáte**[43]**.**

[38] Obsah technickej dokumentácie produktu s digitálnymi prvkami je uvedený v prílohe VII, Nariadenia 2024/2847.
[39] Obsahy EÚ vyhlásenia o zhode a zjednodušeného vyhlásenia o zhode sú uvedené v prílohách V a VI, Nariadenia 2024/2847.
[40] Postup kontroly stanovený v prílohe VIII, Nariadenia 2024/2847.
[41] Postup kontroly stanovený v prílohách VIII a VII, Nariadenia 2024/2847.
[42] Postup kontroly stanovený v prílohe VIII, Nariadenia 2024/2847
[43] Formát technickej dokumentácie v zjednodušenej podobe pre MSP zverejní EK v priebehu roka 2025.

1.8.4 Sankcie

Súčasťou Nariadenia CRA je aj výška sankcií za neplnenie ustanovení tohto nariadenia. Každý členský štát má tak právo uplatniť sankcie v nasledujúcich prípadoch:

- V prípadoch, ak výrobca, dovozca, distribútor alebo správca softvéru s otvoreným zdrojovým kódom neplní základné požiadavky kybernetickej bezpečnosti produktu, môže dostať správnu pokutu do výšky 15.000.000,- EUR alebo do 2,5 % jeho celosvetového ročného obratu za predchádzajúci rok, podľa toho, ktorá suma je vyššia.
- V prípadoch, ak výrobca, dovozca, distribútor alebo správca softvéru s otvoreným zdrojovým kódom poruší ustanovenia týkajúce sa vyhlásenie zhody produktu s európskymi normami, nemá v požadovanom stave technickú dokumentáciu alebo má chyby ohľadom označovania produktu značkou CE, môže dostať správnu pokutu do výšky 10.000.000,- EUR alebo do 2 % jeho celosvetového ročného obratu za predchádzajúci rok, podľa toho, ktorá suma je vyššia.
- V prípadoch ak výrobca, dovozca, distribútor alebo správca softvéru s otvoreným zdrojovým kódom poskytne nesprávne alebo neúplne informácie orgánom dohľadu alebo notifikovanej osobe, môže dostať správnu pokutu do výšky 5.000.000,- EUR alebo do 1 % jeho celosvetového ročného obratu za predchádzajúci rok, podľa toho, ktorá suma je vyššia.

2 Regulačné prostredie na úrovni SR

Kybernetickú bezpečnosť v podmienkach Slovenskej republiky upravujú predovšetkým dva dokumenty. Prvým je zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý je transpozíciou Nariadenia NIS2 do slovenského právneho systému, druhým je potom dokument „Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025“, určujúci komplexný prístup SR k zaisteniu kybernetickej bezpečnosti.

2.1 Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

Zákon č. 69/2018 Z. z. (ďalej zákon) o kybernetickej bezpečnosti bol novelizovaný zákonom č. 366/2024 Z. z.[44] v novembri 2024, s účinnosťou od 1. januára 2025.[45] **Predmetom novelizácie bola transpozícia smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na vysokú spoločnú úroveň kybernetickej bezpečnosti v Únii (NIS2) do slovenského právneho systému.**

Novela zákona rozširuje rozsah pôsobnosti zákona na nové odvetvia a subjekty, ktoré sú považované za dôležité z hľadiska kybernetickej bezpečnosti. Novela tiež zavádza nové požiadavky na kybernetickú bezpečnosť pre dotknuté subjekty, vrátane povinnosti implementovať opatrenia na riadenie rizík a oznamovať incidenty. Zákon o kybernetickej bezpečnosti takisto upresňuje tie časti Nariadenia NIS2, ktoré podľa znenia tohto európskeho dokumentu mali upraviť jednotlivé členské štáty EÚ.

2.1.1 Dohliadajúci orgán

Slovenská právna úprava v prvom rade určuje v oblasti kybernetickej bezpečnosti hlavný dohliadajúci orgán, ktorým je **Národný bezpečnostný úrad** (ďalej NBÚ). V rozsahu svojej pôsobnosti však môžu vykonávať úlohy v oblasti kybernetickej bezpečnosti aj jednotlivé ministerstvá, ako aj iné orgány štátnej správy (napr. Úrad na ochranu osobných údajov alebo Najvyšší kontrolný úrad). NBÚ v pozícií ústredného orgánu má definované úlohy a právomoci, ku ktorým mimo iné patrí aj vykonávanie dohľadu nad podnikateľskými subjektami, právo udeľovať sankcie, ale aj vydávanie certifikácie kybernetickej bezpečnosti na „vysokej“ úrovni. Zároveň pôsobí ako schvaľujúci orgán pre oprávnené osoby vydávajúce certifikáty na úrovniach „základná“ a „významná“ a aj ako akreditačný orgán pre jednotky CSIRT, zriadené u podnikateľských subjektov.

NBÚ je prevádzkovateľom **Národného centra kybernetickej bezpečnosti** (ďalej NCKB)**[46],** ktoré plní na národnej úrovni úlohu **jednotného kontaktného miesta.** NCKB naviac plní úlohy **národnej jednotky CSIRT**, čo znamená, že je hlavným kontaktným bodom pre riešenie kybernetických incidentov na národnej úrovni. Týka sa to všetkých podnikateľských subjektov, vrátane tých, ktoré sú definované ako kritické. Tu je však nutné podotknúť, že zodpovednosť za jednotlivé kritické podniky môžu niesť aj CSIRT tímy príslušných ministerstiev.[47] V prípade, ak je dohľad realizovaný týmto spôsobom, sektorové jednotky CSIRT sú povinné spolupracovať s národnou jednotkou.

[44] https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101.html
[45] https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/?ucinnost=01.01.2025
[46] https://www.sk-cert.sk/sk/aktuality/index.html
[47] Sektorová príslušnosť kritických podnikov je uvedená v prílohách 1 a 2, zákona č. 69/2018 Z.z.:
https://static.slov-lex.sk/pdf/prilohy/SK/ZZ/2018/69/20250101_5701664-2.pdf
https://static.slov-lex.sk/pdf/prilohy/SK/ZZ/2018/69/20250101_5701666-2.pdf

NCKB na svojom webovom sídle prevádzkuje **Jednotný informačný systém kybernetickej bezpečnosti.**[48] Systém súži ako centrálna platforma pre zhromažďovanie, spracovanie a výmenu informácií o kybernetických hrozbách a incidentoch. Okrem metodických usmernení vedie register ústredných orgánov s kompetenciami v oblasti kybernetickej bezpečnosti, register kritických subjektov, zoznam akreditovaných jednotiek CSIRT, ako aj aktuálne výstrahy pred známymi kybernetickými hrozbami. **Zároveň obsahuje webové rozhranie pre nahlasovanie kybernetických incidentov**[49]**, určené (nielen) pre subjekty, ktoré tak podľa tohto zákona musia konať.**

2.1.2 Rozsah pôsobnosti

V pôsobnosti zákona sú poskytovatelia kritických **základných služieb** usadení v SR tak, ako sú zaradení do odvetvového **zoznamu subjektov** v prílohách 1 a 2 tohto zákona[50], ktoré sú zároveň **subjektmi na úrovni stredných (a väčších) podnikov**. Naopak, subjekty poskytujúce verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu, správcovia domén najvyššej úrovne, poskytovatelia služieb názvov domén, poskytovatelia dôveryhodných služieb, subjektov od ktorých sú závislé kritické služby konkrétneho sektora alebo akékoľvek tretie strany s vplyvom na zaisťovanie kybernetickej bezpečnosti **spadajú do pôsobnosti zákona bez ohľadu na svoju veľkosť.**

Slovenská právna úprava po novelizácií nerozlišuje rozdelenie na kľúčové a dôležité subjekty, ako je tomu v Nariadení NIS2 a zavádza kategórie základných služieb a kritických základných služieb. V praxi však ide len o terminologickú zmenu a odvetvové, aj pododvetvové členenie dotknutých podnikov je prakticky identické s Nariadením NIS2.

Výnimky z tohto zákona sú takisto v súlade s Nariadení NIS2. Ide o nasledujúce prípady:

- **Subjekty, ktoré poskytujú služby organizáciám verejnej správy** pôsobiacim v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, odhaľovania a stíhania trestných činov, môžu byť z pôsobnosti tohto zákona vyňaté. V takom prípade sa riadia príslušnou vnútroštátnou legislatívou.
- **Výskumné inštitúcie,** najmä ak ich činnosť má charakter vedeckého výskumu a experimentálneho vývoja, môžu byť z pôsobnosti tohto zákona vyňaté, ak o tom rozhodne dohliadajúci orgán alebo orgán štátnej správy s takouto kompetenciou.
- **Prevádzkovatelia databáz osobných údajov** sú povinné riadiť sa nielen ustanoveniami tohto zákona, ale predovšetkým podmienkami stanovanými v Nariadení o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (GDPR).
- **Subjekty sprostredkovateľských služieb, hostingových služieb a online platforiem** sú povinné riadiť sa nielen ustanoveniami tohto zákona, ale predovšetkým podmienkami stanovanými v špeciálnom európskom odvetvovom Nariadení o digitálnych službách (DSA).
- Subjekty **finančných služieb** sú povinné riadiť sa nielen ustanoveniami tohto zákona, ale predovšetkým podmienkami stanovanými v špeciálnom európskom odvetvovom Nariadení o digitálnej prevádzkovej odolnosti finančného sektora (DORA).
- Subjekty vyrábajúce a ponúkajúce na trhu **výrobky alebo služby s digitálnymi prvkami** sú povinné riadiť sa nielen ustanoveniami tohto zákona, ale predovšetkým podmienkami

[48] https://www.nbu.gov.sk/jednotny-informacny-system-kybernetickej-bezpecnosti/
[49] https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html
[50] https://static.slov-lex.sk/pdf/prilohy/SK/ZZ/2018/69/20250101_5701664-2.pdf
https://static.slov-lex.sk/pdf/prilohy/SK/ZZ/2018/69/20250101_5701666-2.pdf

stanovanými v špeciálnom európskom odvetvovom Nariadení o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (CRA).

- **Partnerské podniky**, ktoré majú od svojej (zahraničnej) protistrany izolovaný systém IKT, môžu byť na základe posúdenia NBÚ vyradené zo zoznamu kritických subjektov na základe nedosiahnutí kritérií stredného podniku.
- NBÚ má právo zaradiť do zoznamu kritických subjektov akýkoľvek **malý podnik (alebo mikropodnik)** s významným dosahom na kybernetickú bezpečnosť kľúčového subjektu, organizácie verejnej a štátnej správy alebo ozbrojených zložiek.

Zoznam poskytovateľov kritických základných služieb musí NBÚ zostaviť do 17.4.2025 a následne zverejniť v registri kritických subjektov webového sídla Jednotného informačného systému kybernetickej bezpečnosti.

2.1.3 Povinnosti poskytovateľov základnej služby

Ak poskytovateľ základnej služby zistí, že prekročil tzv. dopadové kritériá nutné pre registráciu kritických subjektov, musí registráciu vykonať najneskôr **do 60 dní** podaním formulára[51] Národnému bezpečnostnému úradu. Subjekt je povinný tak urobiť **z vlastnej iniciatívy**, bez vyzvania dohliadajúceho orgánu. Pre **pomoc so samoidentifikáciou** subjektu ako ne/poskytovateľa kritickej základnej služby, je na webovom sídle NBÚ zriadená online **indikatívna pomôcka** (dotazník s vyhodnotením)[52].

Poskytovateľ základnej služby musí **do 12 mesiacov po zápise do registra prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia,** s cieľom zabezpečiť kybernetickú bezpečnosť a odolnosť. Bezpečnostnými opatreniami sa podľa § 20 zákona rozumie:

- určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
- detekcia kybernetických bezpečnostných incidentov,
- evidencia kybernetických bezpečnostných incidentov,
- postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
- určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
- pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania,
- určenie a pridelenie úloh, rolí a zodpovednosti podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly,
- určenie konkrétnej osoby alebo konkrétnych osôb zodpovedných za schvaľovanie bezpečnostných opatrení, dohľad, kontrolu a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie,
- vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.

[51] https://www.nbu.gov.sk/oznamenie-o-zapise-do-registra-prevadzkovatelov-zakladnej-sluzby/

[52] https://nis2.nbu.gov.sk/indikativna-pomocka-na-urcenie-subjektu-ako-poskytovatela-zakladnej-sluzby/?csrt=3905626245589749343

V prípade, ak sa na subjekt vzťahujú **sektorové bezpečnostné opatrenia**, musí ich taktiež dodržiavať.

Ak poskytovateľ základnej služby využíva na činnosti súvisiace s **prevádzkou sietí a informačných systémov tretie strany**, musí vykonať analýzu rizík dodávateľského reťazca a so spolupracujúcou protistranou uzatvoriť **zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností**.

Subjekt je podľa zákona povinný vytvoriť **mechanizmus informovania vedenia spoločnosti** o kybernetických hrozbách, zraniteľnostiach a incidentoch. V prípade, ak dôjde **k bezpečnostnému incidentu,** subjekt je povinný takú udalosť **okamžite nahlásiť dohliadajúcemu orgánu**, **poskytnúť mu úplnú súčinnosť pri riešení incidentu** a v prípade ak má subjekt podozrenie na **trestnú činnosť** musí **zabezpečiť dôkazy** a **informovať orgány činné v trestnom konaní**.

Správcovia TLD a subjekty poskytujúce služby registrácie názvu domén majú podľa zákona povinnosť pri registrácii domény **evidovať a viesť osobitnú evidenciu registračných údajov.** Táto musí obsahovať: **názov domény, dátum jej registrácie, meno a priezvisko alebo názov držiteľa domény,** jeho **kontaktné údaje** (elektronickú adresu a telefónne číslo), resp. aj **kontaktné údaje žiadateľa o registráciu,** ak je iný ako držiteľ domény. **Overovanie** údajov pri registrácií musí prebiehať na základe **interných predpisov a postupov** a musí obsahovať najmenej verifikáciu mena a priezviska alebo názov držiteľa domény. Po registrácii domény je nutné **bezodkladne a bezplatne zverejniť údaje**, ktoré nie sú osobnými údajmi.

Oba typy subjektov sú tiež povinné **najneskôr do 72 hodín sprístupniť registračné údaje**, ak o to požiada dohliadajúci orgán alebo iný orgán štátnej správy. V súvislosti s tým musia **na svojom webe zverejniť vnútorné predpisy** a informácie o postupoch pri poskytovaní údajov.

Povinnosti vo vzťahu k hláseniu hrozieb a incidentov a reakcií na ne sa v slovenskej právnej norme neodchyľujú od povinností uvedených v Nariadení NIS2. Zákon však presnejšie definuje problematiku vykonávania bezpečnostných **auditov** u prevádzkovateľov základných služieb. Títo musia vykonať audit **do 2 rokov od zaradenia do registra** prevádzkovateľov základných služieb alebo po každej **významnej zmene** bezpečnostných opatrení.

Nekritickí prevádzkovatelia môžu nahradiť audit **samohodnotením** cez Jednotný informačný systém kybernetickej bezpečnosti, avšak **raz za 5 rokov** musia absolvovať aj plnohodnotný audit. Subjekty sú potom povinné predložiť **záverečnú správu z auditu**, spolu s prípadnými **nápravnými opatreniami,** do **30 dní od jeho ukončenia.**

Zákon č. 69/2018 Z. z. takisto upravuje povinnosti subjektov, ak prevádzkujú vlastný tím CSIRT. V takomto prípade sú povinní zabezpečiť, že **interná jednotka CSIRT počas celej doby svojej prevádzky spĺňa podmienky akreditácie NBÚ a bezodkladne oznamuje všetky zmeny, ktoré majú vplyv na túto akreditáciu.** Ak jednotka CSIRT vykonáva dohľad nad **subjektom finančného trhu, vyžiada si vyjadrenie Národnej banky Slovenska** k postupu ústredného orgánu pri plnení úloh podľa tohto zákona.

2.1.4 Dohľad a sankcie

Podmienky dohľadu a s nimi súvisiace presné výšky sankcií, sú v nadriadení NIS2 prenechané na rozhodnutie členských štátov. Slovenská republika tak detailne upravila dohľad, ako aj sankčný mechanizmus, práve v novelizovanom zákone č. 69/2018 Z. z.. **V nasledujúcom prehľade sú vybrané tie ustanovenia, ktoré by sa mohli dotýkať aj MSP**.

Ak je subjekt podrobený kontrole, musí dohliadajúcemu orgánu poskytnúť úplnú a bezpodmienečnú súčinnosť. V prípade, že dohliadajúci orgán SR zistí v činnosti subjektu nedostatky, má právo od prevádzkovateľa základnej služby žiadať vykonanie auditu kybernetickej bezpečnosti, prijatie opatrení na nápravu, poskytnúť verejné informácie o situácií dotknutým stranám a **v krajnom prípade** aj **pozastaviť výkon funkcie vedeniu** spoločnosti, resp. **zakázať poskytovať službu** do času nápravy nevyhovujúceho stavu. Súbežne s týmito opatreniami môže NBÚ uplatniť aj finančný postih v podobe **penále**, v maximálnej výške **35,- EUR za každý deň omeškania plnenia povinností**.

Ak **pri výkone dohľadu** zistí dohliadajúci orgán **konkrétne** porušenie povinnosti uloženej zákonom, má právo popri opatreniach na nápravu uložiť subjektu **pokutu** do výšky **10.000,- EUR**, a to aj opakovane.

V prípade, ak boli porušené povinnosti, ktoré napĺňajú skutkovú podstatu správneho deliktu, dohliadajúci orgán má právo udeliť v tejto veci **aj správnu pokutu (od 300,- EUR do 500.000,- EUR).**

Ak neexistuje iný dôvod na pokračovanie výkonu dohľadu a subjekt je ochotný a schopný nevyhovujúci stav služby odstrániť, ako aj primerane nahradiť vzniknutú škodu, dohliadajúci orgán má možnosť navrhnúť subjektu **uzatvorenie dohody o náprave**. Po uzavretí dohody bude režim dohľadu ukončený.

Kontrolovanému subjektu, ktorý naopak znemožňuje kontrolu alebo marí jej výsledok a nápravu nedostatkov, môže NBÚ uložiť **poriadkovú pokutu** do **1.500,- EUR**, a to aj opakovane, až do úhrnnej výšky 15.000,- EUR.

Priestupkové konanie so sankčným rozsahom od **100,- EUR do 5.000,- EUR** bude podľa zákona uplatňované len voči fyzickým osobám, ktoré:

- porušia mlčanlivosť v súvislosti s plnením úloh podľa toho zákona,
- poskytnú nepravdivé údaje, pri registrácií subjektu ako kritického poskytovateľa služby,
- po registrácií porušia dvanásťmesačnú lehotu na implementáciu bezpečnostných opatrení,
- pri spolupráci s treťou stranou neuzatvoria náležitú dohodu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností alebo ak by to znemožňovalo plnenie dohody, neinformujú tretiu stranu o hlásenom kybernetickom incidente,
- neplnia zákonom dané povinnosti v prípade kybernetického incidentu[53],
- porušili technické, organizačné alebo personálne opatrenia prevádzkovateľa základnej služby,
- zadajú vykonanie auditu kybernetickej bezpečnosti necertifikovanému subjektu,

[53] § 19, ods. 6, zákona č. 69/2018 Z. z.

- nezabezpečia korektné splnenie zákonom daných povinností[54] pri výkone auditu kybernetickej bezpečnosti samohodnotením prostredníctvom Jednotného informačného systému kybernetickej bezpečnosti.

V prípade udeľovania **pokút za správne delikty** má NBÚ zo zákona rozsiahle právomoci.

Finančnú sankciu **od 300,- EUR do 500.000,- EUR** môže udeliť **prevádzkovateľovi základnej služby**, ak podľa § 31 odseku 1 zákona poruší povinnosť:

- oznámiť začiatok vykonávania činnosti podľa § 17 ods. 2,
- oznámiť zmenu údajov podľa § 17 ods. 6 alebo
- oznámiť prevádzkovanie kritickej základnej služby podľa § 18 ods. 2,
- podľa § 19 ods. 2 až 4, ods. 6 písm. f) alebo ods. 7,
- udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa § 20 ods. 3,
- podľa § 29 ods. 1, 2, 5 alebo ods. 8,
- vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29 alebo
- uloženú úradom podľa § 29j ods. 1, alebo **subjekt, spadajúci do pôsobnosti toho zákona** na výzvu NBÚ neoznámi zmenu údajov[55], alebo, ak subjekt neposkytne informácie orgánu štátnej správy, neposkytne súčinnosť a informácie orgánom verejnej moci v súvislosti s kybernetickým incidentom a ak používa konkrétny produkt, službu, postup, či kooperujúci subjekt v rozpore s obmedzujúcim rozhodnutím dohliadajúceho orgánu, alebo, ak podľa § 31 odseku 6 zákona **správca TLD** alebo **poskytovateľ služieb registrácie názvu domén** poruší povinnosť:
- viesť osobitnú evidenciu registračných údajov názvu domény podľa § 22 ods. 1,
- prijať vnútorné predpisy, zaviesť osobitné postupy na zabezpečenie overenia údajov predkladaných pri registrácii názvu domény a ich zverejniť podľa § 22 ods. 3,
- sprístupniť údaje predkladané pri registrácii názvu domény podľa § 22 ods. 4 alebo
- poskytnúť úradu alebo ústrednému orgánu údaje podľa § 22 ods. 5. alebo, ak **výrobcovia** alebo **poskytovatelia produktov, služieb alebo procesov, ktoré sú certifikované**, majú vydané EÚ vyhlásenie o zhode v rozpore so schémou certifikácie kybernetickej bezpečnosti [56], alebo, ak vyššie uvedení výrobcovia a poskytovatelia (vrátane tých, ktorým už bolo vydané EÚ vyhlásenie o zhode) v elektronickej podobe nezverejnia alebo neaktualizujú doplňujúce informácie o kybernetickej bezpečnosti [57] alebo, ak **držiteľ certifikátu kybernetickej bezpečnosti** neposkytne NBÚ informácie, potrebné na plnenie úloh úradu, znemožní NBÚ vykonať bezpečnostný audit alebo znemožní NBÚ prístup do svojich priestorov.

Finančnú sankciu **od 300,- EUR do 7.000.000,- EUR alebo do výšky 1,4 % celkového svetového obratu za predchádzajúci rok (podľa toho, ktorá suma je vyššia),** môže NBÚ udeliť prevádzkovateľovi **základnej služby**, ak podľa § 31 odseku 2 zákona poruší povinnosť:

- podľa § 19 ods. 1 alebo ods. 6 písm. a) až e) alebo písm. g) až i),
- prijať bezpečnostnú dokumentáciu podľa § 20 ods. 3,
- nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 alebo ods. 3,

[54] § 29, ods. 8, zákona č. 69/2018 Z.z.
[55] Podľa § 21 ods. 3, zákona č. 69/2018 Z.z.
[56] Podľa Nariadenia (EÚ) 2019/881, čl. 49 ods. 7.
[57] Podľa Nariadenia (EÚ) 2019/881, čl. 55 ods. 1, písm. a) až d).

- zasielať automatizovaným spôsobom určené systémové informácie podľa § 24a ods. 1,
- 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 alebo
- predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8.

Prevádzkovatelia **kritickej základnej služby** za uvedené porušenia podľa § 31 odseku 2 zákona môžu od NBÚ dostať pokutu **od 500,- EUR do 10.000.000,- EUR alebo do výšky 2 % celkového svetového obratu za predchádzajúci rok (podľa toho, ktorá suma je vyššia)**.

V prípade, ak príde do roka k opakovanému porušeniu povinností, za ktoré už raz bola udelená finančná sankcia, má NBÚ právo udeliť pokutu až do výšky dvojnásobku vyššie uvedených súm.

2.2 Národná stratégia kybernetickej bezpečnosti na roky 2021-2025

Národná stratégia kybernetickej bezpečnosti na roky 2021–2025 je **strategickým dokumentom**, ktorý vypracovalo Ministerstvo investícií, regionálneho rozvoja a informatizácie SR. Tento dokument definuje na uvedené obdobie rámec pre zabezpečenie kybernetickej bezpečnosti štátu, súkromných subjektov, ale aj jednotlivcov. Cieľom stratégie je zlepšiť ochranu kybernetických systémov, infraštruktúry a dát na národnej úrovni a podporiť spoluprácu medzi verejným a súkromným sektorom.

Dokument je rozdelený do viacerých kapitol, ktoré sú venované rôznym aspektom kybernetickej bezpečnosti. Bližšie sa zameriavajú na súčasný stav, strategické ciele, konkrétne opatrenia a ich implementáciu.

Úvodná kapitola vo všeobecnosti definuje základné princípy kybernetickej bezpečnosti, definuje hlavné legislatívne a inštitucionálne rámce tak na európskej, ako aj domácej úrovni a stanovuje okruhy cieľov a priorít.

V ďalšej časti sa zameriava na celkový stav kybernetickej bezpečnosti v SR k obdobiu vzniku dokumentu, vrátane krátkeho popisu najbežnejších bezpečnostných hrozieb alebo stavu legislatívy a vymáhania práva.

Dokument pokračuje kapitolami, venovanými zahraničnopolitickému kontextu kybernetickej bezpečnosti, mechanizmom pre monitorovanie a hodnotenie pokroku, ako aj postupom uplatňovaným pre revíziu stratégie na základe aktuálneho vývoja. Krátka záverečná kapitola je potom venovaná otázkam financovania programov kybernetickej bezpečnosti, s dôrazom na štát a jeho organizácie.

Z pohľadu podnikateľských subjektov je však najrelevantnejšou kapitolou tá najobsiahlejšia, venujúca sa **strategickým cieľom a opatreniam na ich dosiahnutie**. Aj napriek staršiemu dátumu vzniku tohto dokumentu, ostávajú niektoré z nich aktuálne dodnes.

Okrem okruhov venovaných strategickým cieľom štátu a verejnej správy, cieľom v oblastiach odhaľovania a objasňovania kybernetickej kriminality alebo zámerom rozvíjania

medzinárodných partnerstiev, či výskumu a vývoja, sú spomenuté aj ciele a opatrenia na podporu zodolnenia súkromného sektora alebo prípravy kvalitných odborníkov.

Základné ciele pre súkromný sektor, s dôrazom na poskytovateľov základných služieb, sú v Národnej stratégii definované v podobe **napĺňania adresných sektorových bezpečnostných požiadaviek**, ktoré doplnia už zavedené minimálne nároky na kybernetickú bezpečnosť alebo **systematické zvyšovanie povedomia** prevádzkovateľov základných služieb a kritickej infraštruktúry. Tretím cieľom je vytvorenie bázy pre **efektívnu spoluprácu verejného a súkromného sektora**, nielen v oblasti regulácie, ale aj v zdieľaní informácií a skúseností a v ďalšom rozvoji.

Pre splnenie týchto cieľov je podľa dokumentu treba prijímať opatrenia na **prispôsobenie prístupu k jednotlivým sektorom** podľa ich špecifických potrieb, **poskytovanie podpory** prevádzkovateľom základných služieb a kritickej infraštruktúry **pri implementácii bezpečnostných opatrení** a **rozvoj spolupráce**, výmeny informácií a odbornej diskusie medzi verejným a súkromným sektorom.

V oblasti prípravy **odborníkov na kybernetickú bezpečnosť,** dokument konštatuje, že v praxi je ich citeľný nedostatok. Súvisí to predovšetkým s absenciou špecificky zameraných vysokoškolských programov a s tým súvisiacou absenciou adekvátne pripravených učiteľov. Dokument ďalej konštatuje, že na trhu je viacero odborných kurzov a školení, ktoré sa však problematike venujú len ad hoc. Cieľom by teda malo byť zabezpečenie kvalitného **vysokoškolského odborného vzdelávania** v oblasti kybernetickej bezpečnosti, ako aj rozvoj **špecializovaného vzdelávania** ako formy celoživotného vzdelávania. Na to je potrebné vytvorenie systému odborného vzdelávania na vysokých aj stredných školách a schém podpory **špecializovaného vzdelávania** pre už existujúcich odborníkov.

V súvislosti so systematickou univerzitnou prípravou odborníkov na kybernetickú bezpečnosť je potrebné podotknúť, že dnes, takmer päť rokov po prijatí aktuálnej národnej stratégie, je situácia v tejto oblasti výrazne lepšia. Dedikované **študijné programy zamerané na kybernetickú bezpečnosť je možné študovať** na viacerých verejných a súkromných školách (napríklad Fakulta informatiky a informačných technológií Slovenskej technickej univerzity, Fakulta bezpečnostného inžinierstva Žilinskej univerzity, Technická univerzitu v Košiciach a iné.)

2.3 Najdôležitejšie zmeny pre MSP od 1.1.2025

Nové kategórie regulovaných subjektov

Pokým do 1.1.2025 spadali do účinnosti zákona len poskytovatelia základných a digitálnych služieb z oblasti energetiky, dopravy, zdravotníctva alebo bankovníctva, novela upravuje povinnosti pre omnoho širšiu skupinu podnikateľských subjektov. Ak podnik spĺňa aspoň jedno z kritérií (50 a viac zamestnancov alebo minimálny ročný obrat 10 miliónov EUR) je po novom povinný sa **registrovať ako prevádzkovateľ základnej služby**. Táto povinnosť sa novo vzťahuje aj na menšie podniky, ak ich činnosť podľa zákona spĺňa kritéria kritickej služby. Podniky, ktoré sa samoidentifikújú ako prevádzkovatelia základnej služby, sú **povinné zapísať sa do 60 dní** do registra takýchto subjektov, ktorý vedie NBÚ.

Prísnejšie bezpečnostné opatrenia

Pred novelou mali dotknuté spoločnosti povinnosť zaviesť iba základné bezpečnostné opatrenia. Malé a stredné podniky, ktoré spadajú do pôsobnosti novelizovaného zákona majú po 1.1.2025 povinnosť plniť prísnejšie požiadavky na riadenie kybernetických rizík, monitorovanie incidentov a zavádzanie pokročilejších bezpečnostných mechanizmov. Všetky opatrenia musia vykonávať najmenej v rozsahu, ako explicitne ustanovuje novelizované znenie zákona.

Všetky MSP, na ktoré sa novelizácia vzťahuje, sú naviac povinné do 12 mesiacov implementovať bezpečnostné opatrenia na základe analýzy rizík, a spracovať ich formu bezpečnostnej dokumentácie. MSP, ktoré poskytujú kritickú základnú službu, sú povinné do 24 mesiacov preveriť účinnosť týchto opatrení prostredníctvom auditu kybernetickej bezpečnosti, ktorý vykonáva certifikovaný audítor. MSP, ktoré poskytujú len základnú službu, smú vykonať namiesto auditu sebahodnotenie, avšak do piatich rokov sú takisto povinné podrobiť sa certifikovanému auditu.

Reportovanie incidentov

Do novelizácie zákona bolo hlásenie kybernetických incidentov povinné len pre prevádzkovateľov základných služieb alebo poskytovateľov digitálnych služieb. Od 1.1.2025 **musia kybernetické incidenty hlásiť všetky subjekty**, vrátane tých MSP, ktoré spĺňajú odvetvové alebo veľkostné kritériá zaradenia do pôsobnosti nového znenia zákona.

Prísnejšie sankcie

Novelou boli zavedené vyššie pokuty pre širší okruh subjektov, opäť vrátane MSP, ktorých sa novela dotýka. V priestupkovom konaní je možné subjektom uložiť pokuty v širokom spektre maximálnych výšok, a to podľa porušenia daného ustanovenia zákona. V prípade nesúladu s konkrétnou povinnosťou, je finančná sankcia do 10.000,- EUR. V prípade správneho deliktu poskytovateľa základnej služby môže byť udelená pokuta až do 500.000,-EUR, avšak v prípade vážnejších deliktov až do výšky 7.000.000,- EUR. Poskytovatelia kritickej základnej služby sú v prípade správneho deliktu vystavení hrozbe pokuty až do 10.000.000,- EUR.

Presná výška finančných sankcií, ako aj deliktov, za ktoré môžu byť udelené, je podrobne spracovaná v kapitole *2.1 Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, časti 2.1.4 Dohľad a sankcie.*

3 Príklady implementácie opatrení v praxi

Zámerom tejto kapitoly je poskytnúť prehľad o vybraných dobrých príkladoch z praxe zavádzania opatrení pre posilňovanie kybernetickej bezpečnosti v rámci krajín EÚ. Rovnako kapitola zahŕňa aj najčastejšie chyby a nedostatky, ktoré môžu zvyšovať riziko negatívnych dôsledkov potenciálnych kybernetických útokov. V neposlednom rade je z týchto príkladov vybraných niekoľko prístupov, uplatniteľných aj v slovenských podmienkach.

Transpozícia smernice NIS2 do vnútroštátnej legislatívy členských štátov EÚ, je spojená s určitou mierou flexibility, ktorá umožňuje zohľadniť špecifiká národného prostredia. Nižšie sú zosumarizované hlavné požiadavky a spôsob, akým by mali byť prevzaté.

NIS2 požiadavky	Povinné	Flexibilné
Pokrytie sektorov a subjektov	nutnosť dodržiavať rozsah NIS2	žiadne zmeny nie sú povolené
Manažment kybernetických hrozieb	minimálne 7 hlavných bezpečnostných opatrení	nemôže byť menej
Reportovanie incidentov (24h, 72h, 1 mesiac)	povinné pre všetky vymedzené subjekty	žiadna flexibilita
Dohľad nad kybernetickou bezpečnosťou a sankcie	povinnosť udeľovať sankcie (max 10mil./2 % obratu)	možnosť definície vlastných mechanizmov
Národná stratégia kybernetickej bezpečnosti	požadovaná	možnosť flexibilného uchopenia
Osveta verejnosti a školenia	nepožadovaná	plne na členskom štáte
Bezpečnosť dodávacích reťazcov	požadovaná principiálne	možnosť flexibilného uchopenia
Certifikačné štandardy	nepožadované	plne na členskom štáte

3.1 Pozitívne príklady z iných členských štátov EÚ

V definíciách národných regulácií tak možno nájsť naprieč EÚ rozdiely, a teda aj prístupy, ktoré môžu byť niečím efektívnejšie a účinnejšie.

Dánsko

Dánsko má ku kybernetickej bezpečnosti výrazne proaktívny postoj, čo sa odráža aj v transpozícii smernice NIS2 do vnútroštátneho práva a jeho pokročilom implementačnom úsilí. Okrem iného zaviedlo Dánsko povinné programy školení v oblasti kybernetickej bezpečnosti pre zamestnancov v kľúčových sektoroch. Citeľne zlepšilo zdieľanie informácií o kybernetických hrozbách v reálnom čase medzi podnikmi a vládnymi orgánmi. MSP zároveň dostávajú finančnú podporu a stimuly na investovanie do kybernetickej bezpečnosti. Hlavné benefity teda možno vidieť v:

- lepšie pripravenej pracovnej sile - redukované ľudské chyby vedúce k kybernetickým útokom,
- efektívnejších mechanizmoch kybernetickej obrany - podniky proaktívne monitorujú hrozby,
- lepšej ochrane pre MSP, ktoré sú často najzraniteľnejšie.

Slovensko môže pri implementácii NIS2 čerpať inšpiráciu práve v zavedení programov a školení v oblasti kybernetickej bezpečnosti pre zamestnancov v kľúčových sektoroch, aby vedeli napr. spoľahlivejšie rozpoznávať phishingové útoky a ďalšie bezpečnostné riziká.

Do úvahy pripadá tiež poskytnutie finančných stimulov pre MSP, ako sú daňové úľavy alebo granty na investovanie do opatrení kybernetickej bezpečnosti. Tie je možné podporiť implementáciou nástroja na hodnotenie rizík kybernetickej bezpečnosti pre MSP, aby mohli posúdiť svoju vlastnú bezpečnostnú situáciu, čím by sa zároveň systematicky a prakticky zvyšovalo povedomie o kybernetických hrozbách.

Belgicko

Belgicko už v súčasnosti dokončilo svoje vnútroštátne vykonávacie akty pre smernicu NIS2, čím vytvorilo robustný právny rámec na riešenie výziev kybernetickej bezpečnosti. Zaviedlo národné audity kybernetickej bezpečnosti, aby zabezpečilo, že podniky spĺňajú stanovené bezpečnostné normy. Spoločnosti vďaka tomuto prístupu efektívnejšie ohlasujú kybernetické incidenty, čo vedie k rýchlejším reakciám vlády. Rovnako nastavilo finančné stimuly, kedy sektory kritickej infraštruktúry dostávajú štátnu podporu na prevenciu kybernetických útokov.

Hlavné benefity sú v:

- rýchlejšom odhaľovaní a reakciách na hrozby,
- zlepšenej národnej kybernetickej odolnosti - menej úspešných kybernetických útokov na kľúčové odvetvia,
- lepšej spolupráci medzi verejným a súkromným sektorom.

Podobne ako Belgicko, Slovensko v rámci implementácie NIS2 zavádza povinné audity kybernetickej bezpečnosti pre kľúčové sektory na zabezpečenie súladu s reguláciou a hladšej adopcie požiadaviek dotknutými subjektmi. Dôležité je, aby priebeh a zameranie týchto auditov bolo efektívne, praktické a nie samoúčelné.

Významnou praktickou pomocou je zriadenie mechanizmu rýchleho ohlasovania incidentov, ktorý štandardizuje a zefektívni postup a tým dokáže citeľne skrátiť čas od vzniku po nahlásenie kybernetických útokov a zvýšiť dodržiavanie predpisov spoločnosťami.

Na prehĺbenie a posilnenie partnerstiev medzi verejným a súkromným sektorom, môže Slovensko vytvoriť nástroje, ktoré podnikom uľahčia zdieľať poznatky o kybernetickej bezpečnosti s vládou.

Okrem už uvedených pozitívnych dopadov, tieto kroky prispejú k zníženiu rizika regulačných pokút pre spoločnosti (čo opäť prispeje lepšej kooperácii) a podniky získajú prístup k odbornému poradenstvu na zlepšenie kybernetickej bezpečnosti (samozrejme za predpokladu, že štát bude disponovať požadovanou odbornosťou a kapacitami).

Chorvátsko

Chorvátsko patrí medzi jeden z mála členských štátov EÚ, ktoré dokončili a prijali vnútroštátnu legislatívu na transpozíciu smernice NIS2, čím preukázali záväzok k posilneniu opatrení kybernetickej bezpečnosti.

Práve skorá transpozícia znamená, že podniky a vládne agentúry majú viac času na prispôsobenie sa a implementáciu osvedčených postupov. Vláda v Chorvátsku poskytuje bezpečnostné usmernenia špecifické pre jednotlivé sektory, čo uľahčuje podnikom dodržiavanie predpisov. MSP a poskytovatelia digitálnych služieb dostávajú štruktúrované školenia v oblasti kybernetickej bezpečnosti.

Hlavné výhody spočívajú v:

- nižšej miere regulačnej neistoty - spoločnosti vedia, čo sa od nich vyžaduje;
- dostatočnom čase, dostupnom pre podniky na implementáciu požadovaných bezpečnostných zmien;
- znížených nákladoch na dodržiavanie predpisov, vďaka postupnej implementácii, namiesto náhlych zmien.

Inšpirujúc sa pozitívnym dopadom včasnej implementácie v Chorvátsku, Slovensko môže podnikom umožniť postupné fázy adoptovania NIS2, aby neboli zahltené kompletným rozsahom bezpečnostných požiadaviek v krátkom čase. Rovnako môže poskytnúť výnimky pre malé podniky a zjednodušené bezpečnostné pravidlá pre MSP, ktoré nie sú súčasťou kritickej infraštruktúry. MSP sa tak môžu na zmeny pripraviť v zvládnuteľnom tempe a spoločnosti nečelia ťažšie plánovateľným nákladom na dodržiavanie predpisov na poslednú chvíľu.

Maďarsko

Maďarsko prijalo nový zákon o kybernetickej bezpečnosti a zodpovedajúce vykonávacie vládne nariadenie 1. januára 2025, čím účinne transponovalo základnú smernicu NIS2 do vnútroštátneho práva. Organizácie, na ktoré sa vzťahuje nový právny rámec, sa museli zaregistrovať u určeného dozorného orgánu pre kybernetickú bezpečnosť do júna 2024, čím sa zabezpečil štruktúrovanejší prístup k dodržiavaniu predpisov.

Vďaka tomuto prístupu majú spoločnosti v Maďarsku včasné a jasné usmernenia týkajúce sa požiadaviek na kybernetickú bezpečnosť, čo znižuje zmätok a neskoré zabezpečenie dodržiavania predpisov. Včasná registrácia na druhej strane umožňuje orgánom identifikovať organizácie s vysokým rizikom a ponúknuť podporu ešte pred vznikom incidentov. Vládny dohľad ďalej zabezpečuje, že kritické sektory (financie, energetika, zdravotníctvo) majú definované proaktívne stratégie kybernetickej bezpečnosti.

Hlavné identifikované prínosy sú v:

- silnejšej kultúre kybernetickej bezpečnosti naprieč podnikmi,
- nižšom riziku kybernetických útokov, vďaka štruktúrovaným, povinným bezpečnostným protokolom,
- lepšej koordinácii reakcie na incidenty s vládnymi agentúrami.

Ako vhodné opatrenie, aj v podmienkach Slovenska, sa javí zavedenie procesu včasnej registrácie pre spoločnosti, na ktoré sa NIS2 vzťahuje, aby si vedeli jednoducho, spoľahlivo a v dostatočnom predstihu potvrdiť, či musia dodržiavať predpisy. Túto požiadavku môže adresovať práve zrozumiteľný a dobre odkomunikovaný spôsob samoidentifikácie subjektov. Ďalšou inšpiráciou je vytvorenie odvetvových špecifických usmernení, ktoré uľahčia dodržiavanie predpisov pre odvetvia ako zdravotníctvo, financie a IT. Ako už bolo spomenuté vyššie v kontexte Dánska, hodnotným praktickým riešením by bol centralizovaný portál

kybernetickej bezpečnosti, kde si podniky môžu skontrolovať svoj stav súladu s reguláciou, nahlásiť incidenty a získať prístup k praktickým odporúčaniam a osvedčeným postupom.

Celkovo teda možno pozitívne skúsenosti z iných členských štátov zhrnúť do niekoľkých kľúčových východísk, na ktoré by sa mal klásť pri implementácii dôraz:

- jasnejšie regulačné požiadavky vedú k lepšiemu dodržiavaniu predpisov a menším právnym rizikám,
- spolupráca vlády a podnikov prispieva k lepšej národnej koordinácii kybernetickej bezpečnosti,
- silnejšia ochrana MSP (financovanie, školenia a jasné usmernenia) pomáhajú menším podnikom zlepšiť bezpečnosť,
- zákazníci aj partneri sa cítia bezpečnejšie pri spolupráci s podnikmi, ktoré dodržiavajú predpisy, čo zvyšuje celkovú dôveru v digitálne služby.

3.2 Najväčšie výzvy a chyby pri implementácii

1. Nedostatočné hodnotenie rizika a nesprávna identifikácia zahrnutých subjektov

Mnoho podnikov nedokáže správne posúdiť svoje riziká kybernetickej bezpečnosti a určiť, či spadajú pod NIS2. Niektorí predpokladajú, že sú oslobodení, hoci sa v skutočnosti kvalifikujú ako kľúčové alebo dôležité subjekty. Odporúčaním je:

- vykonávať pravidelné hodnotenia rizík s cieľom určiť vystavenie kybernetickým hrozbám,
- použiť jasné národné usmernenia, ktoré pomôžu podnikom pochopiť, či sa na ne NIS2 vzťahuje,
- v prípade neistoty, či sa na vykonávanú činnosť vzťahuje NIS2, použiť na webovom sídle NBÚ indikatívnu pomôcku vo forme online dotazníka s vyhodnotením.

2. Pristupovanie k NIS2 ako k jednorazovej úlohe zhody

Niektoré organizácie považujú NIS2 za jednorazovú povinnosť namiesto toho, aby integrovali kybernetickú bezpečnosť do svojej každodennej prevádzky a vytvorili dlhodobé bezpečnostné stratégie. Odporúčaním je:

- namiesto jednorazového projektu, zavádzať nepretržitý proces zlepšovania kybernetickej bezpečnosti,
- neuspokojiť sa s minimálnym požadovaným riešením zabezpečenia kybernetickej bezpečnosti a investovať do komplexného systému, berúc v úvahu aj špecifiká sektoru,
- vykonávať pravidelné audity, školenia a aktualizácie zabezpečenia, aby podniky zostali v súlade.

3. Nedostatok školenia a povedomia zamestnancov

Zamestnanci sú často najslabším článkom kybernetickej bezpečnosti. Spoločnosti investujú do technických riešení, ale nedokážu efektívne vyškoliť zamestnancov v oblasti phishingu, sociálneho inžinierstva a bezpečných hesiel. Odporúčaním je:

- implementovať priebežné školenia v oblasti kybernetickej bezpečnosti pre zamestnancov na všetkých úrovniach;
- vykonávať simulované phishingové útoky na testovanie informovanosti zamestnancov.

4. Neadekvátne plánovanie reakcie na incidenty

Spoločnosti nemajú jasný plán reakcie na kybernetické incidenty. Keď dôjde k porušeniu, prepadnú panike, čím sa oneskorí reakcia a často aj zhorší rozsah dôsledkov útoku. Odporúčaním je:

- vypracovať podrobný plán reakcie na incidenty, ktorý obsahuje postupy:
  - na koho sa v prípade útokov obracať (interné/externé tímy),
  - aké kroky podniknúť na obmedzenie a zmiernenie útoku,
  - komunikačné protokoly (zákazníci, úrady, partneri).
- vykonávať pravidelné cvičenia v oblasti kybernetickej bezpečnosti na testovanie reakcieschopnosti.

5. Slabá bezpečnosť dodávateľa a dodávateľského reťazca

Spoločnosti sa zameriavajú iba na svoju vlastnú bezpečnosť a ignorujú riziká na úrovni dodávateľov a tretích strán. Útoky na dodávateľský reťazec (napr. SolarWinds, Kaseya) pritom využívajú práve slabé stránky externých poskytovateľov a partnerov. Odporúčaním je:

- vykonávať pravidelné hodnotenia bezpečnosti všetkých dodávateľov a partnerov;
- požadovať od dodávateľov, aby dodržiavali osvedčené postupy v oblasti kybernetickej bezpečnosti (napr. MFA, šifrovanie a pod.);
- implementovať politiku nulovej dôvery na obmedzenie externého prístupu k citlivým systémom.

6. Nenahlásenie incidentov včas

Mnohé organizácie odkladajú oznamovanie kybernetických incidentov regulačným orgánom. Strach z poškodenia dobrého mena vedie niektoré podniky k tomu, aby skrývali porušenia, čím sa jednak zvyšujú tresty, no predovšetkým sa odďaľuje alebo úplne znemožňuje poučenie z konkrétneho útoku naprieč širším podnikateľským prostredím. Odporúčaním je:

- dodržiavať 24-hodinové pravidlo počiatočného hlásenia NIS2 pre významné incidenty kybernetickej bezpečnosti,
- definovať jasný interný proces pre notifikovanie orgánov a dotknutých zákazníkov.

7. Prehliadanie úrovne zabezpečenia cloudu a režimu vzdialenej práce

Spoločnosti sa spoliehajú na cloudové služby, ale nekonfigurujú ich bezpečne. Zamestnanci pracujúci z domova/vzdialene používajú slabé heslá, nezabezpečené domáce siete alebo osobné zariadenia anepoužívajú dvojfaktorové autentifikácie. Odporúčaním je:

- používať viacfaktorové overenie (MFA) pre všetky vzdialené prihlásenia;
- používať VPN zabezpečenie pri pristupovaní k údajom, serverom, aplikáciám a pod. vzdialene;
- šifrovať citlivé údaje uložené v cloude;
- implementovať nástroje zabezpečenia koncových bodov pre vzdialených zamestnancov.

8. Ignorovanie ľudského faktora v kybernetickej bezpečnosti

Spoločnosti sa príliš zameriavajú na technické riešenia (firewally, antivírusy), ale ignorujú ľudské správanie, ľahkú manipulovateľnosť a náchylnosť podľahnúť aj menej sofistikovaným hrozbám. Útoky sociálneho inžinierstva pritom zostávajú jednou z najväčších hrozieb. Odporúčaním je:

- implementovať prísne kontroly oprávnení (obmedzovanie prístupu ku kritickým systémom či dátam),
- školiť zamestnancov, ako rozpoznať a nahlásiť podozrivú aktivitu.

9. Podceňovanie potreby zdrojov na dodržiavanie predpisov

Podniky hospodária s obmedzenými zdrojmi a preto prioritizujú výdavky, pri ktorých očakávajú najväčší pozitívny dopad. . Rozpočet na kybernetickú bezpečnosť tak často ostáva nedostatočný a takéto spoločnosti nedokážu najať kvalifikovaných odborníkov, resp. prijať adekvátne opatrenia na predchádzanie hrozbám. Obmedzené IT zdroje sa pritom obzvlášť dotýkajú MSP. Odporúčaním je:

- plánovať priebežné investície do kybernetickej bezpečnosti, nielen počiatočné náklady na dodržiavanie predpisov,
- outsourcing služieb kybernetickej bezpečnosti, ak chýbajú interné odborné znalosti.

10. Nesúlad s inými predpismi (GDPR, DORA atď.)

Spoločnosti často neprepájajú NIS2 reguláciu s existujúcimi požiadavkami GDPR, DORA alebo ISO 27001. To vedie k duplicitnému úsiliu, dodatočným nákladom a neefektívnosti. Odporúčaním je:

- zosúladiť NIS2 s požiadavkami GDPR na ochranu údajov,
- použiť medzinárodné bezpečnostné štandardy (ISO 27001, NIST) na vytvorenie jednotného prístupu.

4 Kvalitatívny prieskum

Súčasťou analýzy bola realizácia kvalitatívneho prieskumu, zameraného na zhodnotenie vnímania a reálnej praxe problematiky kybernetickej bezpečnosti. Forma prieskumu bol riadený, štruktúrovaný rozhovor, uskutočnený vo väčšine prípadov vzdialene, prostredníctvom online video hovoru. Rozhovorom predchádzala mailová komunikácia, ktorá stručne oboznámila respondentov s kontextom a zámerom rozhovoru a taktiež vymedzila hlavné okruhy diskusie, aby mali oslovené spoločnosti priestor na prípravu, resp. zozbieranie vstupov od relevantných osôb. Diskutované okruhy boli nasledovné:

- Je vo vašej firme oblasť kybernetickej bezpečnosti systematicky zastrešovaná?
- Pokiaľ nie, aké sú dôvody, prečo sa vo firme systematicky nevenujete oblasti kybernetickej bezpečnosti?
- Aké sú naopak primárne dôvody, kvôli ktorým riešite tému kybernetickej bezpečnosti?
- Akou formou je kybernetická bezpečnosť vo vašej firme inštitucionalizovaná?
- Aké zdroje vaša firma alokuje na riešenie kybernetickej bezpečnosti (zamestnanci, IT implementácia, externé služby a pod.)?
- Ako vo vašej firme prebieha reportovanie a riešenie bezpečnostných incidentov?
- Máte vo firme skúsenosť s narušením bezpečnosti? Ak áno, aké (povaha, pôvod, rozsah škôd, prípadné prijaté opatrenia/odporúčania a pod.)?
- Ktoré kybernetické hrozby považujete za najväčšie?
- Ako by ste zhodnotili pripravenosť a odolnosť vašej firmy voči kybernetickým hrozbám?
- Čo považujete za najväčšie prekážky, ktoré bránia lepšej pripravenosti vašej firmy?
- Ako máte definované pravidlá a popísané procesy práce s dátami, ich tokov, ukladania atď.? Máte vo firme dedikovaného DPO?
- Ako máte definované pravidlá a popísané procesy pri vytváraní zákazníckych a zamestnaneckých profilov, kont a pod.?
- Ako pristupujete k revízii procesu zbierania súhlasov?
- Ako vnímate rolu štátu pri tvorbe legislatívneho rámca a vytvárania podmienok pre efektívnejšie uchopenie kybernetickej bezpečnosti?
- Čo by podľa vás mohol štát urobiť lepšie alebo odlišne z pohľadu regulácie kybernetickej bezpečnosti a vytvárania čo najvhodnejšieho prostredia?
- Akú podporu vo všeobecnosti by ste vo vzťahu k zvyšovaniu kybernetickej bezpečnosti považovali za účinnú?

Samotné rozhovory prebiehali v zmysle nasledovnej šablóny:

- Stručné predstavenie zúčastnených;
- Sumarizácia cieľov a okolností prieskumu (vrátane zdôraznenia anonymity);
- Diskusia k jednotlivým vymedzeným okruhom;
- Priestor pre dodatočné otázky a diskusiu;
- Záverečné zhrnutie a poďakovanie.

Prieskum bol vykonaný na vzorke 16 vybraných malých a stredných podnikateľov. V tejto vzorke boli zahrnutí podnikatelia z rôznych odvetví, aby bolo možné získať pestrejší a komplexnejší pohľad do ich uvažovania a pristupovania k danej problematike. Išlo predovšetkým o nasledovné odvetvia:

- obchod;
- služby;
- IT sektor;
- poradenské a finančné služby ;
- výroba.

Z hľadiska pôsobenia, ide o firmy podnikajúce prevažne v rámci územia Slovenskej republiky, viaceré však majú aj zahraničný presah. Zamestnávajú pritom rôzne počty zamestnancov, od najmenších (do 5 zamestnancov) až po firmy do 249 zamestnancov.

Všetky z dopytovaných spoločností majú skúsenosti s digitálnymi technológiami, ktoré im pomáhajú s rôznymi aspektami ich podnikateľskej činnosti:

- Logistika;
- Účtovníctvo a finančné riadenie;
- Marketingové a e-commerce riešenia;
- HR softvér;
- CRM systémy;
- Dodávateľské-odberateľské riešenia;
- Zákaznícke informačné systémy.

Zároveň je možné konštatovať, že v digitálnych technológiách firmy vidia veľký potenciál a prínos, no nie vždy im podmienky a okolnosti umožňujú ich využitie do takej miery, akú by považovali za adekvátnu. Hlavnými vnímanými prekážkami sú pritom nedostatočné finančné možnosti a personálne kapacity.

4.1 Formalizácia prístupu ku kybernetickej bezpečnosti

Napriek využívaniu digitálnych technológií a každodennému kontaktu s internetom a online prostredím, v niektorých prípadoch až kritickej závislostí firiem od ich dostupnosti, kybernetická bezpečnosť nezohráva v povedomí manažmentu a priori poprednú rolu. Miera inštitucionalizácie kybernetickej ochrany naberá podobu od úplného nezáujmu (kedy odpoveďou na otázku, či je problematika bezpečnosti v dotknutej spoločnosti systematicky zastrešovaná bolo strohé "nie") až po prepracovaný, profesionálny systém (kedy sa naopak respondent oprel o pomocnú otázku "ako hlboko mám zachádzať?").

U firiem, ktoré v rozhovoroch deklarovali žiadne, resp. minimálne aktívne riadenie bezpečnosti na úrovni IKT, tento stav koreluje s nízkym záujmom a znalosťou danej problematiky. Uvedené sa pritom netýka len malých firiem, ktoré sa necítia byť terčom cielených útokov (neuvedomujúc, resp. podceňujú potenciálne hrozby plošného charakteru), ale aj väčších firiem. Na druhej strane však hodnotia pripravenosť/odolnosť firmy voči kybernetickým hrozbám ako nedostatočnú. V rozhovoroch tieto firmy na otázku, či je oblasť kybernetickej bezpečnosti systematicky zastrešovaná odpovedali "okrajovo", "čiastočne", resp. "v rámci IT agendy".

Firmy s formalizovaným prístupom ku kybernetickej bezpečnosti využívajú na organizačnej úrovni dedikovanú osobu, prípadne s narastajúcou veľkosťou aj celý organizačný útvar. Preto aj ich odpoveď ohľadom systematického zastrešenia bola pohotovo kladná. Vo väčšine prípadov disponujú dobre popísanými bezpečnostnými postupmi a smernicami, ktoré sa snažia medzi zamestnancami šíriť prostredníctvom vstupných a pravidelných školení. Tento

prístup dobre ilustruje odpoveď "snažíme sa v rámci možností preniesť na zamestnancov aspoň také povedomie, ktoré zabráni kliknutiu na zjavný fraudulentný odkaz". Taktiež sa čiastočne spoliehajú na externých partnerov, resp. bezpečnosť poskytovanú ako súčasť rozličných softvérových balíkov a platených riešení. V tejto súvislosti respondenti vyjadrovali očakávanie v duchu "keď už si platím softvérový balík, hádam mi prinesie aj adekvátne zabezpečenie". Sofistikovanejšie spoločnosti potom bezpečnosti venujú aj vlastný softvérový vývoj.

Hlavnou pohnútkou firiem pritom nie je samotná regulácia a požiadavky, ktoré na ne kladie. Jednoznačne najväčší prínos, ktorý pripisujú ochrane pred útokmi, je v podobe redukcie možných finančných a materiálnych škôd a považujú ju principiálne za automatickú súčasť oblasti IKT. Respondenti opakovane, trochu inými slovami, odkazovali na výšku finančných strát, ktoré zachytili vo svojom okolí alebo médiách a boli spôsobené práve hackerskými útokmi. V prenesenejšej forme, opatreniami si firmy snažia chrániť svoju reputáciu, ktorá nemusí predstavovať bezprostredné ohrozenie ich aktív, ale môže v strednodobom horizonte spôsobiť významnejšie straty.

Z pohľadu zdrojov, ktoré firmy približne alokujú na zastrešenie kybernetickej bezpečnosti (zamestnanci, IT implementácie, dodávané externé služby a pod.), tieto ani u jednej nepresahujú v pomere k tržbám hranicu 5 %. Práve financie sú jeden z limitujúcich faktorov, ktorý (adekvátne veľkosti firme) prispieva menšej pripravenosti na prípadné útoky, a ktorý zástupcovia dopytovaných spoločností uvádzali ako jednu z hlavných prekážok pre ďalšie zlepšovanie odolnosti. Diskusia pri prvej otázke ohľadom výšky dostupných zdrojov obvykle začala so slovami "nemáme priamo vyhradený rozpočet", "kybernetickej ochrane špecificky venujeme minimum prostriedkov", "je to jedna z mojich mnohých agend, sporadicky kúpime nejaké zariadenie, raz sme v súvislosti s GDPR riešili externé školenie". Obzvlášť pri menších spoločnostiach, rezonoval problém nedostatku času, vychádzajúci z nutnosti, resp. nastavenia zameriavať sa interne predovšetkým na obchodné a prevádzkové aspekty podnikania. Zároveň tieto firmy nie sú pripravené investovať významnejšie čiastky ani do jednorazových aktivít, čo ilustrujú vyjadrenia ako "neexistuje, aby som niekomu zaplatil tisíce za školenie a o mesiac mohol školiť opäť nových ľudí", "sústredíme sa na biznis, maximálne čo riešime sú účtovníci, tí nám občas radia aj v právnych záležitostiach a upozornia, keď sa nás týka nejaká legislatívna zmena".

4.2 Proces riešenia incidentov

Najmenšie firmy s najnižšou mierou formalizácie oblasti kybernetickej bezpečnosti nemajú vypracované žiadne procesy pre manažment bezpečnostných incidentov. Ich prax tak pozostáva z čisto reaktívneho prístupu, v rámci ktorého vedenie firmy podľa rozsahu útoku/škôd spätne zisťuje, čo presne sa stalo a ako je tomu možné do budúcna predísť. Neopierajú sa pritom o žiadne dedikované nástroje, ani externú expertízu. Diskusia bola v tomto prípade do značnej miery abstraktná, pokiaľ v spoločnosti nemali priamu skúsenosť s narušením bezpečnosti, respondenti operovali v rovine "riešili by sme to ako akýkoľvek iný problém, väčšinou to skončí u mňa a ja následne obvolávam dodávateľov alebo hľadám spôsob, ako zabezpečiť nápravu".

Bežným postupom pri väčších firmách je pri riešení incidentov využívanie služieb externých dodávateľov. Ide pritom buď priamo o dodávateľov konkrétnych používaných softvérových a hardvérových riešení, ale taktiež spoločnosti, zabezpečujúce výhradne bezpečnostné služby - tzv. bezpečnostné operačné centrá (SOC). Pre túto skupinu vystihuje situáciu vyjadrenie jedného zo zástupcov "na incidenty vo všeobecnosti máme definované postupy, v tomto smere mám pomerne vysokú dôveru v to, že zamestnanci by vedeli na koho sa obrátiť".

K podpore typicky pristupujú niekoľkými spôsobmi:

- priamy kontakt na príslušnú zodpovednú osobu na strane dodávateľa;
- zadávanie tiketu v dohodnutom aplikačnom prostredí;
- využívanie kompetencií zodpovednej osoby, ktorá je prvým kontaktným bodom;
- v najprepracovanejšej podobe štandardizovaný postup na reportovanie v súlade s ISO 27001.

Aj u firiem s dobre definovanými a popísanými procedúrami však v diskusiách zástupcovia poukazovali na nedôslednosť, resp. kolísavé vnímanie naliehavosti zastrešovania témy kybernetickej bezpečnosti. Čerstvá skúsenosť s útokom výrazne zvyšuje pozornosť aj alokované zdroje, no s časovým odstupom rýchlo opadá. Ako odznelo v jednom z rozhovorov "zíde z očí, zíde z mysle, napätie ktoré bolo vtedy okolo témy bezpečnosti u nás cítiť už rozhodne nepretrváva".

4.3 Ochrana dát

Každá zo spoločností zapojených do analýzy, v určitom rozsahu pristupuje k dátam, na ktoré sa vzťahuje ochrana pri ich spracúvaní. Kým vo viacerých prípadoch možno hovoriť skôr o minimalistickej forme (napr. na úrovni zamestnaneckých údajov), v jednom prípade spoločnosť systematicky vyhodnocuje zákaznícke správanie sa, čím jej dokonca vzniká povinnosť určenia zodpovednej osoby (DPO). Táto spoločnosť pritom využíva služby externého DPO, ktorý na seba preberá súvisiace zodpovednosti a disponuje zároveň poistkou. Pokiaľ firmy nemajú povinnosť ustanoviť DPO, na dobrovoľnej báze inklinujú prirodzene k internej pozícii, pretože na ňu kladú nižšie nároky a z pohľadu prevádzkových nákladov je ekonomickejšia. U malých firiem bol však názor podobný, "nevieme si dovoliť takejto oblasti vyhradiť celú pozíciu, máme to zahrnuté v rámci právnych služieb, kde verím že na to externá firma, ktorá celú právnu oblasť zastrešuje, dostatočne dôsledne myslí".

Hoci veľkosť vzorky a metodika dopytovania neumožňujú formulovať kvantitatívne závery, je zároveň zaujímavé, že vymenovanie DPO nekorelovalo jednoznačne s veľkosťou spoločností. Interná pozícia sa vyskytla aj u firmy s 21-50 zamestnancami, naopak absentovala pri firme so 151-250 zamestnancami (pôsobiacej v obchode). Všetky firmy s DPO deklarovali jasne definované pravidlá a popísané procesy práce s dátami, vrátane ich tokov, spôsobov ukladania a pristupovania k nim a pod. Takáto úroveň manipulácie s dátami bola dostupná aj pri spomínanej väčšej firme, hoci bez prítomnosti dedikovaného DPO.

Na explicitne položenú otázku ohľadom dostupnosti jasne definovaných pravidiel a popísaných procesov pri vytváraní zákazníckych a zamestnaneckých profilov, odpovedali kladne opäť len tie firmy, ktorým oblasť zastrešuje DPO, v opačnom prípade bola odpoveď aj v tomto prípade "nie", resp. v jednom z rozhovorov aj s dôvetkom "načo by sme to robili?".

Rovnako väčšina z dotknutých spoločností pravidelne reviduje a aktualizuje formu a obsah zbierania súhlasov od zákazníkov. Absencia obdobných postupov pritom obzvlášť pri väčších spoločnostiach naznačuje, že GDPR v povedomí manažmentu nemá adekvátnu prioritu, a to napriek pomerne intenzívnej komunikácii, ktorá implementáciu regulácie sprevádzala. Situácia je lepšia pri firmách, pôsobiacich v online prostredí, kde sa napr. nástroje na monitoring cookies postupne stali bežnou súčasťou a vplývajú nutne aj na povedomie samotných podnikateľov.

Celkovo je v kontexte spracúvania osobných údajov a ochrany dát možné zhodnotiť, že prítomnosť DPO vo firme citeľne zvyšuje mieru sofistikovanosti pri nakladaní s údajmi, zároveň však túto potrebu firmy nepociťujú rovnomerne.

4.4 Najväčšie vnímané hrozby

Zástupcovia zapojených spoločností identifikovali v diskusiách nasledovné kybernetické hrozby:

- phisingové útoky,
- napadnutie cloudových služieb a úložísk,
- ransomware,
- malware,
- zneužitie hesiel/krádež identity,
- používanie vlastných zariadení zamestnancami,
- interné úniky dát,
- DDoS útoky,
- nezabezpečené siete mimo pracovísk.

Práve phisingové útoky a napadnutie cloudových služieb a úložísk odznievali opakovane ("nevyžiadané maily evidujeme neprestajne", "zrovna pred pár dňami dostali viacerí kolegovia správu ohľadom doručovania nejakej zásielky", "na telefónoch si dnes už viete jednoducho blokovať číslo, nerozumiem prečo to nevedia rovnako blokovať aj tu"), predstavujú teda z pohľadu podnikateľov najväčšie vnímané aktuálne kybernetické hrozby. Ich výskyt považujú za pomerne pravdepodobný, viacerí preto v záujme predchádzať škodám relatívne aktívne pristupujú k edukácii zamestnancov (a dokonca výnimočne aj k simulácii útoku).

Výraznejšiu obavu spôsobuje taktiež ransomware, najmä z dôvodu priamych škôd, ktoré potenciálne dokáže podnikateľom napáchať ("u nás disponujeme hodnotnou bázou dát ohľadom zákazníkov a ich správania, keby sa k nej niekto neoprávnene dostal, bol by to veľký problém"). Naopak nikto z respondentov neuviedol možnosť napadnutia slabých článkov v rámci dodávateľských reťazcov, napriek tomu, že vykazuje rastúci trend a na úrovni EÚ je táto hrozba považovaná za významnú.

Vo všeobecnosti si podnikatelia na jednej strane kybernetické hrozby uvedomujú a v hlbšej diskusii rozoznávajú narastajúce schopnosti (a možnosti) útočníkov, na strane druhej si však menej pripúšťajú možnosť, že práve oni sa stanú ďalšími obeťami útoku. Niekoľkí menší podnikatelia v rozhovore parafrázovane uviedli "prečo by niekto útočil práve na nás?".

4.5 Skúsenosti s narušením bezpečnosti

Žiaden z respondentov neuviedol bezprostrednú skúsenosť s útokom, ktorý by označil za signifikantný, teda so zásadným dopadom na prevádzkyschopnosť spoločnosti a jej služieb, financie, resp. kompromitujúci osobné alebo citlivé dáta ("okrem tých mailov neevidujem, že by sa vo firme za posledné roky niečo obdobné vyskytlo", "zásadnejšiu skúsenosť nemáme"," keby niečo zanechalo finančnú škodu, pamätal by som si"). Väčšina zástupcov počas svojho pôsobenia neevidovalo žiadne narušenie bezpečnosti, prípadne len drobného rozsahu (na úrovni odcudzenia/straty hardvéru a pod.).

U dvoch spoločností bol zaznamenaný v minulosti problém s cielenými nevyžiadanými e-mailami a phisingovými kampaňami, ktoré mali aj negatívnu (hoci nie signifikantne) dohru. V

jednom prípade došlo ku kompromitácii účtu, pričom dôvodom bola nedodržaná dvojfaktorová autentifikácia zamestnancom, avšak žiadne väčšie škody neboli následne zaznamenané a v dôsledku incidentu sa sprísnili pravidlá prihlasovania. V druhom prípade zamestnanec otvoril potenciálne škodlivý súbor v prílohe, ani v tomto prípade však nedošlo k viditeľným negatívnym následkom.

Ďalší respondent sa v spoločnosti stretol s ransomware, ktorý krátkodobo obmedzil poskytované interné služby (uzamknutím operačného systému na virtuálnom serveri). Situáciu sa však podarilo vyriešiť dodávateľsky a využitím dobre nastaveného systému zálohovania. V nadväznosti na dané narušenie bezpečnosti, zaviedli vo firme nutnosť využívania zabezpečenej VPN pre vzdialené pristupovanie na daný server.

Posledným konkrétnym zlyhaním bezpečnosti bol nedostatočne chránený kontaktný webový formulár, ktorý bol napadnutý DDoS útokom a spôsobil krátkodobé znefunkčnenie webu.

Je pochopiteľné, že rozsah opatrení, ktoré podnikatelia prijímajú vo vzťahu ku kybernetickej bezpečnosti je primeraný ich veľkosti a ekonomickým možnostiam, dá sa však pozorovať prístup, ktorý je skôr reaktívny.

4.6 Vnímanie roly štátu

Podnikatelia považujú štát za signifikantného aktéra, obzvlášť pri tvorbe legislatívneho rámca a vytváraní podmienok pre efektívnejšie uchopenie kybernetickej bezpečnosti, no majú zároveň pocit, že si svoju rolu plní nanajvýš neutrálne. Sentiment väčšiny respondentov vystihuje jedna z reakcií, kedy zástupca uviedol "na jednej strane sa tu bavíme o zákonoch a ako ich štát môže robiť lepšie, na strane druhej nemám pocit, že by kvalita podnikateľského prostredia bola úprimným záujmom, takže si vo finále nie som istý, či by som vlastne akejkoľvek aktivite dôveroval".

Medzi podnetmi ohľadom toho, čo by mohol štát urobiť inak z pohľadu regulácie kybernetickej bezpečnosti a zlepšovania prostredia podnikatelia uvádzali nasledovné postrehy:

- kvalitnejšie IT prostredie na strane štátu,
- lepšie povedomie o regulácii a požiadavkách, ktoré firmám kladie,
- pravidelné vzdelávacie aktivity,
- aktívnejší dialóg pri tvorbe/adaptovaní regulácie,
- nižšie sankcie.

Najmä kvalita štátneho IT prostredia a taktiež zvyšovanie povedomia v podnikateľskom sektore sú kroky, ktoré rezonujú najsilnejšie a odzneli takmer u každého respondenta. Ako však už odznelo vyššie, tieto návrhy sprevádza zo strany podnikateľov zjavná skepsa a boli formulované trochu silene - "ak musím niečo uviesť, tak asi to povedomie, ale neviem čo by mala byť tá správna platforma, aby sa to aj dostalo k relevantným ľuďom", "keď občas zachytím v akých čiastkach sa pohybujú štátne IT zákazky a porovnám si to s kvalitou, akú vnímam ja z pohľadu zákazníka, je tam obrovský nepomer".

V kontexte drahých verejných obstarávaní a málo hmatateľných výsledkov, majú podnikatelia v štát pomerne nízku dôveru a nevnímajú ho v rámci IT ako dostatočne kompetentného partnera.

4.7 Prekážky a možné príležitosti

V rámci diskusie ohľadom najväčších vnímaných bariér pre zvyšovanie kybernetickej bezpečnosti, respondenti pomerne jednotne označili finančné zdroje. Ako už bolo naznačené, práve tie sú v rámci prioritizácie jednotlivých investičných, či prevádzkových opatrení rozhodujúce a kybernetická bezpečnosť je na vyšších priečkach v princípe najmä vtedy, keď príslušná spoločnosť zažíva, resp. má čerstvú skúsenosť s bezpečnostným incidentom. Z väčšiny rozhovorov však zároveň bolo cítiť aj slabšie povedomie, resp. podceňovanie hrozieb, preto odznievala doplňujúca otázka, či "nie je čiastočne problém aj chýbajúce povedomie a informácie ohľadom kybernetických hrozieb?". V odpovedi niektorí respondenti pripúšťali menšiu znalosť, ale predovšetkým pozornosť, ktorú oblasti venujú. Následná diskusia potom úzko súvisela s osvetou a aktivitami, ktoré aj samotní podnikatelia, resp. manažéri môžu realizovať. Tie pritom nutne nemusia klásť až tak výrazné nároky na financie, preto v diskusii napr. jeden z respondentov reagoval slovami, že "pravdepodobne prepošle phisingový mail na zamestnancov" a skúsi tak zvýšiť ich pripravenosť.

Jeden z respondentov v rozhovore uviedol ako prekážku taktiež zhoršujúcu sa geopolitickú situáciu, ďalší dvojsečnosť narastajúcej závislosti od informačných technológií.

Pri hľadaní vhodných príležitostí, účastníci prieskumu primárne uvažovali v intenciách ich vlastných možností a schopností a až v nadväznosti na otázky ohľadom roly štátu sa niektorí vrátili k idei štátnej podpory. Hlavné príležitosti sú každopádne priamo previazané s najväčšími prekážkami, t. j. akákoľvek forma finančnej pomoci a prístup k relevantným, spoľahlivým a zrozumiteľným informáciám. Viacerí z respondentov pritom finančnú podporu neočakávali nevyhnutne priamu, uvedomujúc si realisticky obmedzené možnosti aj na strane štátu, no poukazovali skôr na prostredie a nástroje, ktoré štát vytvára a spravuje (v tejto súvislosti bol 2x spomenutý útok na kataster). Pri poskytovaní vzdelávania vnímali potenciál silnejšie, avšak 2x s dôvetkom, že "na druhej strane si nie sú celkom istí kompetentnosťou".

Zaujímavým postrehom bola vzájomná spolupráca a zdieľanie dobrej praxe medzi podnikateľskými subjektami. V rozvedenej diskusii potom respondent dospel k názoru, že štát by potenciálne mohol vytvoriť a facilitovať platformu, ktorá by niečo podobné umožňovala.

Záver

MSP sú pomerne výrazne ovplyvnené analyzovanými predpismi a ich dodržiavanie vyžaduje, aby MSP implementovali robustné opatrenia kybernetickej bezpečnosti, čo môže byť náročné na ich finančné aj ľudské zdroje.

MSP, ktoré sa identifikujú ako subjekty spadajúce pod komplex legislatívy kybernetickej bezpečnosti a GDPR, by mali začať auditom súladu s požiadavkami jednotlivých právnych noriem a následne implementovať opatrenia a hlásiť incidenty tak, aby dosiahli súlad a vyhli sa sankciám. Rámcovo je možné najhlavnejšie požiadavky sumarizovať nasledovne:

- Podniky musia v súvislosti s dodržiavaním ustanovení GDPR implementovať opatrenia na ochranu osobných údajov, pravidelne aktualizovať procesy kybernetickej bezpečnosti a školiť zamestnancov v pravidlách GDPR.
- Dotknuté MSP musia podľa CSA a CRA pri výrobe a distribúcií produktov a služieb IKT dodržiavať európske certifikačné schémy kybernetickej bezpečnosti.
- Podniky, na ktoré sa vzťahuje DSA musia zaviesť systém hlásenia zraniteľností produktov a služieb IKT a zabezpečiť ich softvérovú podporu (najmenej po dobu 5 rokov), tak aby zaistili ich dlhodobú kybernetickú bezpečnosť.
- Pre MSP, na ktoré sa nevzťahuje CSA, je z obchodného hľadiska výhodné získať na báze dobrovoľnosti aspoň základný certifikát kybernetickej bezpečnosti.
- MSP, ktoré prevádzkujú web-shopy, online trhoviská, sprostredkovateľské portály, a spravodajské portály, musia podľa DSA zabezpečiť moderovanie obsahu, overovanie obchodníkov, ktorým poskytujú online priestor a zaviesť a dodržiavať pravidlá pre zverejňovanie reklamy.
- MSP pôsobiace v oblasti finančných služieb, musia mať podľa DORA vypracované plány obnovy systémov a musia pravidelne testovať kybernetickú odolnosť infraštruktúry IKT.

Novela zákona č. 69/2018 Z. z. (v podobe zmien uvedených v zákone č. 366/2024 Z. z.) kladie nové povinnosti aj na širšie spektrum malých a stredných podnikov. Osoby zodpovedné v MSP za oblasť kybernetickej bezpečnosti, by nad rámec tohto dokumentu mali preskúmať svoje povinnosti podľa novelizovaného znenia zákona tak, aby sa predovšetkým vzhľadom k svojmu špecifickému odvetvovému zamareniu, dostali do súladu s aktuálnou právnou úpravou.

Niektoré malé a stredné podniky čelia špecifickým problémom, ako sú nízke kybernetické povedomie, nedostatočná bezpečnosť vzdialených IT, vysoké náklady na riešenia v oblasti kybernetickej bezpečnosti a zvýšená úroveň hrozieb, ako je napríklad ransomvér, v súvislosti s ktorými by mali dostať usmernenia a podporu.

Malé a stredné podniky sa čoraz viac stávajú terčom útokov na dodávateľské reťazce z dôvodu ich menej prísnych opatrení na riadenie kybernetických rizík a zvládanie útokov ako aj skutočnosť, že majú obmedzené bezpečnostné zdroje. Takéto útoky na dodávateľské reťazce majú vplyv nielen na malé a stredné podniky a ich izolovanú činnosť, ale môžu mať aj kaskádový účinok na väčšie subjekty, ktorým poskytli dodávky.

Na základe kvantitatívneho prieskumu je pritom možné označiť povedomie a pripravenosť podnikateľského prostredia vo vzťahu ku kybernetickej bezpečnosti za nedostačujúce. Väčšiu váhu zohráva vnímanie hrozieb než samotnej regulácie, no predovšetkým menšie podniky nealokujú v oblasti bezpečnosti adekvátne zdroje. Je vidieť, že intenzívna komunikácia v súvislosti s GDPR mala pozitívny efekt a oblasť ochrany dát je spoločnosťami zastrešovaná na

lepšej úrovni. Národné orgány (ako NBÚ) zohrávajú kľúčovú úlohu pri dohľade nad dodržiavaním predpisov a poskytovaní podpory dotknutým podnikom. Ponúkajú zdroje na samostatnú identifikáciu, registráciu a hlásenie incidentov, no z pohľadu podnikateľského prostredia nie je ich angažovanosť viditeľná.

Štát by mal pracovať na prehĺbení vzťahu s podnikateľským prostredím a snažiť sa zabezpečiť nástroje, ktoré MSP prakticky pomôžu v implementácii potrebných opatrení. Okrem priamej finančnej podpory (ktorá kladie nároky na štátny rozpočet), dokáže štát podnikom pomôcť vhodným časovaním implementácie regulácie a postupným nárokom na zabezpečenie súladu. Kľúčovým je ale aj v tomto prípade dôsledné a efektívne zdieľanie informácií vo forme zrozumiteľnej pre MSP.

Zo zavádzania opatrení pre posilňovanie kybernetickej bezpečnosti v rámci ostatných členských krajín EÚ, je možné identifikovať niekoľko podnetov, prinášajúcich pozitívne výsledky. Jedným z nich je práve silnejšia ochrana MSP (financovanie, školenia a jasné usmernenia), ktorá pomáha najmä menším podnikom zlepšovať bezpečnosť a svoju ochranu.

Je ďalej žiadúce, aby regulačné požiadavky boli formulovanéčo najjasnejším a najzrozumiteľnejším spôsobom, čím sa následne zvyšuje miera ich dodržiavania. Užšia spolupráca vlády a podnikov prehlbuje dôveru a prispieva k lepšej národnej koordinácii kybernetickej bezpečnosti.

Medzi najrozšírenejšie a taktiež najviac vnímané hrozby, patria v súčasnosti phishingové útoky. Ide o príklad narušenia bezpečnosti, ktorý nevyžaduje priame technologické zásahy a investície, keďže je riešiteľný práve prostredníctvom dobrej osvety. Tú však firmy často podceňujú a zamestnanci pri nedostatočnom dôraze na prevenciu sporadicky podľahnú útokom, realizovaným stále sofistikovanejším a presvedčivejším spôsobom. Zmenu v prístupe podnikateľov je možné dosiahnuť vtedy, keď si uvedomia, že úsilie efektívne investované do ochrany pred možnými útokmi, je vo výraznom nepomere voči potenciálnym škodám, ktorým v prípade úspešného útoku môže podnik čeliť.

Zoznam použitej literatúry

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA), Cybersecurity maturity assessment for small and medium Enterprises. 2025. Dostupné na: https://tools.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA). Cybersecurity certification. 2020. Dostupné na: https://www.enisa.europa.eu/sites/default/files/publications/ENISA_candidate%20scheme_EUCC.pdf

SBA, Malé a stredné podnikanie v číslach v roku 2023. Bratislava, 2024. Dostupné na:https://monitoringmsp.sk/wp-content/uploads/2024/05/MSP_v_cislach_2023.pdf

Odporúčanie Komisie č. 2003/361/ES zo 6. mája 2003, ktoré sa týka definície mikro, malých a stredných podnikov. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32003H0361

Európska komisia. Štatistická klasifikácia ekonomických činností – NACE rev. 2. 2008.Dostupné na:https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF

Úrad na ochranu osobných údajov Slovenskej republiky. 2025. Dostupné na: https://dataprotection.gov.sk/sk/

Rada pre mediálne služby. 2025. Dostupné na: https://rpms.sk/

Národný bezpečnostný úrad. 2025. Dostupné na: https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html

Národný bezpečnostný úrad, Jednotný informačný systém kybernetickej bezpečnosti. 2025. Dostupné na: https://www.nbu.gov.sk/jednotny-informacny-system-kybernetickej-bezpecnosti/

Národný bezpečnostný úrad, Oznámenie o vykonávaní činností o poskytovaní služby podľa zákona č. 69/2018 Z. z. 2025. Dostupné na: https://www.nbu.gov.sk/oznamenie-o-zapise-do-registra-prevadzkovatelov-zakladnej-sluzby/

Legislatívne dokumenty:

Zákon č. 366/2024 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. Dostupné na: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/366/20250101

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Dostupné na: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/20250101

Smernica Európskeho parlamentu a Rady č. 2009/73/ES z 13. júla 2009 o spoločných pravidlách pre vnútorný trh so zemným plynom, ktorou sa zrušuje smernica 2003/55/ES. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32009L0073

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 Text s významom pre EHP. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32013R0575

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32012R0648

Nariadenie Európskeho parlamentu a Rady (ES) č. 1907/2006 z 18. decembra 2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemických látok (REACH) a o zriadení Európskej chemickej agentúry, o zmene a doplnení smernice 1999/45/ES a o zrušení nariadenia Rady (EHS) č. 793/93 a nariadenia Komisie (ES) č. 1488/94, smernice Rady 76/769/EHS a smerníc Komisie 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32006R1907R(01)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011. Dostupné na: https://eur-lex.europa.eu/eli/reg/2022/2554/oj?locale=sk

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii). Dostupné na:
https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX:32024R1689

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti). Dostupné na:
https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202402847

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti). Dostupné na:
https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32019R0881

Nariadenie (EÚ) 2022/2065 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách). Dostupné na:https://eur-lex.europa.eu/eli/reg/2022/2065/oj?eliuri=eli%3Areg%3A2022%3A2065%3Aoj&locale=sk